შპს „დენსის“ პერსონალურ მონაცემთა დაცვის პოლიტიკა

“დენსი”

იურიდიული მისამართი:

საქართველო, ქალაქი რუსთავი, კოსტავას გამზ, №11

საქართველო, თბილისი, ყიფშიძის N2ბ

საქართველო, თბილისი, ფანჯიკიძის N22

ახორციელებს სტომატოლოგიური მომსახურების მიწოდებას, სტომატოლოგიურ კლინიკების ქსელ „დენს“-ში

1. შესავალი

1.1 წინამდებარე პოლიტიკის მიზანია უზრუნველყოს კომპანიის პერსონალისა და პაციენტების პერსონალური მონაცემების დამუშავების მიზნების, ძირითადი პრინციპებისა და წესების განსაზღვრება მონაცემთა უსაფრთხოების უზრუნველსაყოფად.

1.2 კომპანია უზრუნველყოფს, რომ მას ქონდეს კონფიდენციალურობის და პერსონალურ მონაცემთა დაცვის სრულყოფილად დანერგილი შიდა წესები/სისტემები, უზრუნველყოს სავალდებულო წესების დაცვა, რომლებიც შესაბამისობაშია მოქმედ კანონმდებლობასთან.

2. პერსონალური მონაცემთა დაცვის პოლიტიკა

2.1. კომპანია პერსონალური მონაცემების დამუშავებასა და დაცვას ახორციელებს **„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნებისა და მონაცემთა დაცვის საერთაშორისო სტანდარტების შესაბამისად.**

2.2. კომპანია იღებს ვალდებულებას, დაიცვას თქვენი პერსონალური მონაცემების კონფიდენციალობა და განმარტავს, თუ როგორ ახორციელებს პირის პერსონალური მონაცემებისა და განსაკუთრებული კატეგორიის პერსონალური მონაცემების შეგროვებას, დამუშავებას, გაზიარებას და დაცვას. პოლიტიკა ასევე განსაზღვრავს პირის უფლებას პერსონალური მონაცემების გამოყენებასთან, წვდომასთან, კორექტირებასა და წაშლასთან დაკავშირებით.

3. წინამდებარე პოლიტიკაში გამოყენებულ ტერმინთა განმარტება.

3.1. წინამდებარე დოკუმენტში გამოყენებული ტერმინები მხოლოდ აღწერილობითია და განმარტებულია სამკურნალო სამუშაო სპეციფიკიდან გამომდინარე. განმარტებები შესაბამისობაშია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან და მათი ინტერპრეტირება კანონის საწინააღმდეგოდ დაუშვებელია;

3.1.2. პერსონალური მონაცემი (შემდგომში - მონაცემი) - ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს და გამოიყენება კომპანიის საქმიანობის მიზნებიდან გამომდინარე;

3.1.3. განსაკუთრებული კატეგორიის მონაცემი - მონაცემი, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს, გამოიყენება კომპანიის საქმიანობის მიზნებიდან გამომდინარე და ავლენს, მათ შორის, ფიზიკური პირის ჯანმრთელობის მდგომარეობას, ნასამართლობის შესახებ ინფორმაციას, ბიომეტრიულ ინფორმაციას;

3.1.4. მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი, რომლის შესახებ არსებული მონაცემი გამოიყენება კომპანიის მიერ საკუთარი მიზნებიდან გამომდინარე. ფიზიკური პირი შესაძლებელია იყოს იდენტიფიცირებული ან იდენტიფიცირებადი;

3.1.5. კომპანია - მონაცემთა დამმუშავებელი, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, მეთოდებს, ფორმებს, ორგანიზაციული და ტექნიკური უსაფრთხოების ზომებს, ასევე, მონაცემთა სუბიექტის უფლებების რეალიზაციის გზებს;

3.1.6. უფლებამოსილი პირი - კომპანიის მიერ, კანონის ან ხელშეკრულების საფუძველზე, მონაცემთა დამუშავების პროცესში ჩართული პირი, რომელიც მონაცემებს ამუშავებს კომპანიის სახელით ან/და მისი მიზნებიდან გამომდინარე. უფლებამოსილ პირად არ ჩაითვლება კომპანიის შრომით ურთიერთობაში მყოფი პირი;
3.1.7. მონაცემთა მიმღები - ნებისმიერი პირი, ვისაც კომპანიის საქმიანობის მიზნებიდან გამომდინარე, გადაეცა პერსონალური მონაცემი, მათ შორის, უფლებამოსილი პირი, კომპანიის ადმინისტრაციის თანამშრომელი, თანაშემწე, სტაჟიორი, აკადემიური და მოწვეული პერსონალი, აბიტურიენტი, სტუდენტი, კურსდამთავრებული;
3.1.8. მონაცემთა დამუშავება - პერსონალური მონაცემის მიმართ განხორციელებული აქტიური ან/და პასიური სახის ნებისმიერი მოქმედება, მათ შორის, ვიდეო და აუდიოკონტროლი. დამუშავება შეიძლება, ასევე, განხორციელდეს სრულად ავტომატური საშუალებებით, ნახევრად ავტომატური ან სრულად მექანიკური საშუალებებით.

4. მონაცემთა დაცვის პოლიტიკის მოქმედების სფერო
4.1 წინამდებარე პოლიტიკა სრულად ვრცელდება კომპანიის მიერ პერსონალური მონაცემების ავტომატური, ნახევრად ავტომატური, ან არაავტომატური საშუალებებით მონაცემთა დამუშავებაზე და გამოიყენება პერსონალური მონაცემთა დაცვის პროცესში.
4.2 აღნიშნული პოლიტიკა ვრცელდება ყველა იმ პირზე, რომელთა მონაცემებიც მუშავდება კომპანიის - სტომატოლოგიური კლინიკების ქსელ „დენსი "-ს მიერ, ასევე, მონაცემთა მიმღებზე და იმ უფლებამოსილ პირებზე, რომლებიც კომპანიის სახელით ან მისთვის ამუშავებენ პერსონალურ მონაცემებს.

5. პერსონალური მონაცემების დამუშავების საფუძვლები და პრინციპები
5.1 კომპანიის მიერ პერსონალური მონაცემების დამუშავება ხდება მხოლოდ შემდეგ შემთხვევებში:
5.1.1. არსებობს მონაცემთა სუბიექტის თანხმობა;
5.1.2. მონაცემთა დამუშავება გათვალისწინებულია კანონით;
5.1.3. მონაცემები საჯაროდ ხელმისაწვდომია;
5.1.4. მონაცემები საჯაროდ ხელმისაწვდომი გახადა თავად მონაცემთა სუბიექტმა;
5.1.5. მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების საფუძველზე მისთვის მომსახურების გაწევის მიზნით;
5.2 მონაცემთა დამუშავება ხდება კონკრეტული პრინციპების შესაბამისად:
5.2.1 სამართლიანობა და კანონიერება - პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, პიროვნების ღირსების შეულახავად;
5.2.2 მკაფიოდ განსაზღვრული კანონიერი მიზნის არსებობა - აუცილებელია, არსებობდეს კონკრეტული მიზანი, რისთვისაც ხდება მონაცემთა დამუშავება. სხვა მიზნებით მონაცემების გამოყენება დაუშვებელია.
5.2.3 პროპორციულობა და ადეკვატურობა - მონაცემები უნდა დამუშავდეს იმ მინიმალური მოცულობით, რაც აუცილებელია მონაცემთა დამუშავების კონკრეტული მიზნის მისაღწევად; თავად მონაცემებიც, ამ მიზნის შესაბამისი უნდა იყოს.
5.2.4 პერსონალური მონაცემების შენახვის ვადა - პერსონალური მონაცემები უნდა ინახებოდეს კანონით განსაზღვრული ვადით ან იმ ვადით, რაც აუცილებელია მიზნის მისაღწევად.

6. პერსონალურ მონაცემთა კატეგორია და მისი დამუშავება
6.1 კომპანია ახდენს ძირითადად რამდენიმე კატეგორიის პერსონალური მონაცემის შეგროვებას და დამუშავებას. კერძოდ:

- **სახელი და გვარი;**
- **პირადი ნომერი ან რომელიმე სხვა საიდენტიფიკაციო დოკუმენტის ნომერი და მისი გამცემი ქვეყანა;**
- **დემოგრაფიული მონაცემები [როგორიცაა, სქესი და დაბადების თარიღი];**
- **ტელეფონის ნომერი;**
- **ელექტრონული ფოსტა;**
- **მისამართი;**
- **საბანკო ანგარიშის მონაცემები და საბანკო ბარათის მონაცემები;**
- **IP მისამართი, რომლის გამოყენებითაც ხორციელდება კომპანიის კუთვნილ ვებსაიტზე შესვლა;**

- **დაზღვევის მონაცემები [როგორიცაა: მომხმარებლის/პაციენტის სადაზღვევო კომპანია, სადაზღვევო პოლისის ინფორმაცია, სადაზღვევო მიმართვა, სადაზღვევო დაფარვა];**
- **მონაცემები ჯანმრთელობის მდგომარეობის შესახებ, როგორიცაა: ცნობები, ისტორია, ანკეტა, დიაგნოზები, რეცეპტები, მედიკამენტური მკურნალობა, ექიმთან ვიზიტები, სხვა;**
- **მონაცემები მომხმარებლის/პაციენტის მიერ სერვისების გამოყენების შესახებ და სერვისების გამოყენებით მომხმარებლის/პაციენტის მიერ ან მომხმარებლისთვის/პაციენტისთვის დანიშნული ვიზიტების შესახებ;**
- **სხვა ინფორმაცია, რომელსაც მომხმარებელი/პაციენტი ნებაყოფლობით გადაწყვეტს, რომ მიაწოდოს კომპანიას [როგორიცაა: ფოტო, სიმაღლე, წონა, ალერგიები, სისხლის ჯგუფი და სხვა], ასევე რომელიც ავტომატურად იგზავნება მონაცემთა სუბიექტთან დაკავშირებული სამედიცინო დაწესებულებიდან და/ან რომლის გამჟღავნებაც ნებაყოფლობით მოითხოვა მონაცემთა სუბიექტმა.**

6.2 პერსონალური მონაცემების დამუშავება გულისხმობს ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით პირის პერსონალური მონაცემების შეგროვებას, ჩაწერას, ფოტოზე აღბეჭდვას, აუდიოჩაწერას, ვიდეოჩაწერას, ორგანიზებას, შენახვას, შეცვლას, აღდგენას.

6.3 თანხმობას მონაცემთა სუბიექტი გამოხატავს ზეპირად, წერილობით, სატელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული წესით, რომლითაც შესაძლებელია დადგინდეს მონაცემთა სუბიექტის ნება და გაკეთდეს შესაბამისი ჩანაწერი.

6.4 კომპანიამ შეიძლება დაამუშაოს მონაცემები მომსახურების საჭიროებიდან გამომდინარე ან განსაკუთრებულ შემთხვევებში სხვა მონაცემთა დამმუშავებლის დახმარებით. მონაცემთა დამუშავება უნდა შეესაბამებოდეს კომპანიის მიერ დადგენილ სტანდარტებს და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს.

7. დამუშავების მიზნები

7.1 კომპანიისთვის მიწოდებული პერსონალური მონაცემების (მათ შორის განსაკუთრებული კატეგორიის მონაცემების) მიზნებს წარმოადგენს: სამედიცინო მომსახურების გაწევა, გასაწევი მომსახურების შესაბამისი სამედიცინო ბარათის წარმოება, სამედიცინო დიაგნოზის დადგენა, პირის სასიცოცხლო ინტერესების დაცვა, საზოგადოებრივი ჯანმრთელობის, ასევე ჯანდაცვის სისტემის ეფექტიანი ფუნქციონირების ინტერესის შესაბამისად მონაცემების დაარქივება, მომსახურების ხარისხის გაუმჯობესება, საჩივრებზე/სარჩელებზე რეაგირება, სამედიცინო მომსახურების გაწევის შედეგად სახელმწიფო, ადგილობრივი ბიუჯეტით დაფინანსებული პროგრამებისა და ქვეპროგრამების განმახორციელებლებიდან, სადაზღვევო ან/და შესაბამისი დამფინანსებლებისგან შესაბამისი ანაზღურების მიღება; შრომით-სამართლებრივი ან/და სხვა სახელშეკრულებო ურთიერთობიდან გამომდინარე ნაკისრი ვალდებულების ჯეროვანი შესრულება.

8. მონაცემებზე წვდომის უფლების მქონე სუბიექტები

8.1.შესაბამისი მიზნისა და პროპორციების ფარგლებში, სამედიცინო ცენტრში დამუშავებულ მონაცემებზე წვდომა საკუთარი კომპეტენციის ფარგლებში შესაძლებელია ჰქონდეს : ადმინისტრატორს, ექიმს, მენეჯერს, რენდგენოლოგს.

9. არასრულწლოვანის შესახებ მონაცემთა დამუშავებაზე თანხმობის გაცემის წესი და პირობები

9.1. არასრულწლოვანის შესახებ მონაცემთა დამუშავება მისი თანხმობის საფუძველზე დასაშვებია, თუ მან 16 წლის ასაკს მიაღწია, ხოლო 16 წლამდე არასრულწლოვანის შესახებ მონაცემთა დამუშავება – მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობით. გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, მათ შორის, როდესაც მონაცემთა დამუშავებისთვის აუცილებელია 16 წლიდან 18 წლამდე არასრულწლოვანისა და მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა.

10. მონაცემთა დამუშავების საფუძვლები

10.1 კომპანია პერსონალურ მონაცემებს ამუშავებს შემდეგი საფუძვლების არსებობისას:

- მონაცემთა სუბიექტის თანხმობის არსებობისას;
- მონაცემთა სუბიექტთან გაფორმებული ხელშეკრულებიდან გამომდინარე, ნაკისრი ვალდებულების შესრულების მიზნით;
- პერსონალურ მონაცემთა დამუშავება გათვალისწინებულია კანონით, ჯანმრთელობის დაცვის შესაბამისი პროგრამით/ადგილობრივი ქვეპროგრამით და სხვა;

- პერსონალურ მონაცემთა დამუშავება საჭიროა პასუხიმგებელი პირის მიერ კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად;
- პერსონალური მონაცემები საჯაროდ ხელმისაწვდომია;
- აუცილებელია სუბიექტის სასიცოცხლო ინტერესების დასაცავად;
- აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად;
- აუცილებელია განცახადების განსახილველად ან მომსახურების გასაწევად.

11. მონაცემთა დამუშავება უფლებამოსილი პირის მიერ

11.1 პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი ვალდებულია დაიცვას პერსონალურ მონამცემთა დაცვის კანონმდებლობა და უზრუნველყოს მის ხელთ არსებული ინფორმაციის კონფიდენციალურობის დაცვა.

11.2 პერსონალურ მონაცემთა დამუშავებაზე უფლებამოსილი პირი ვალდებულია მონაცემების დაამუშავოს მისი კომპეტენციის ფარგლებში და კანონიერი მიზნებიდან გამომდინარე, რაც საჭიროა შრომითი ან/და ვალდებულებით სამართლებრივი ხელშეკრულებით ნაკისრი ვალდებულების ჯეროვანი შესრულებისათვის.

11.3 პერსონალურ მონაცემთა დამუშავებაზე უფლებამოსილ პირს, რომელიც სახელშეკრულებო ურთიერთობიდან გამომდინარე, ახორციელებს პერსონალური მონაცემების დამუშავებას, პასუხისმგებლობა ეკისრება პერსონალურ მონაცემთა გამჟღავნებაზე, უკანონო გამოყენებაზე, დაკარგვაზე, შეცვლაზე, განადგურებაზე და სხვა არაკანონიერ ქმედებებზე.

12. ვიდეოკონტროლისა და აუდიოკონტროლის განხორციელების წესი

12.1 დანაშაულის თავიდან აცილების, მისი გამოვლენის/მოკვლევის, საზოგადოებრივი უსაფრთხოების, პირის უსაფრთხოებისა და საკუთრების დაცვის, საიდუმლო (კონფიდენციალური) ინფორმაციის დაცვის და ლეგიტიმური ინტერესების სფეროსთვის მიკუთვნებული სხვა მნიშვნელოვანი ამოცანების შესასრულებლად, (მათ შორის, ინციდენტების მართვა და მომხმარებელთა უფლებების დაცვა, პროცესების მონიტორინგი, რისკების მართვა და სხვ.) „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი მოთხოვნების დაცვით, ორგანიზაციაში მიმდინარეობს შენობ(ებ)ის გარე და შიდა პერიმეტრის ვიდეო-აუდიო მონიტორინგი ვიდეოსათვალთვალო სისტემის მეშვეობით (შემდგომში - მონიტორინგი).

12.2 მონიტორინგი ხორციელდება 24/7 საათის განმავლობაში, ხოლო ჩანაწერები ინახება 30 კალენდარული დღის ვადით ან/და იმ ვადით, რაც საჭიროა კონკრეტული მიზნის მისაღწევად, რის შემდეგადაც ექვემდებარება ავტომატურ განადგურებას, თუ არ არსებობს მონაცემთა უფრო ხანგრძლივი ვადით შენახვის საჭიროება და სამართლებრივი საფუძველი.

12.3 ინფორმირების უზრუნველსაყოფად, თვალსაჩინო ადგილას განთავსებულია შესაბამისი გამაფრთხილებელი ნიშნები, რომელიც შეიცავს ინფორმაციას როგორც ვიდეო, ასევე, აუდიოჩაწერის თაობაზე.

12.4 კომპანიის მიერ მიღებულია ყველა შესაბამისი ქმედითი და ადეკვატური ორგანიზაციულ-ტექნიკური ზომა, რათა თავიდან იქნეს აცილებული ჩანაწერებში ასახული მონაცემების უკანონო/შემთხვევითი გამჟღავნება, მათი არასასურველი მიზნით გამოყენება, გავრცელება და სხვა, მათ შორის :

ა)უზრუნველყოფილია მონიტორინგის სისტემის ფიზიკური უსაფრთხოება; მონიტორინგის სისტემა და შესაბამისი ტექნიკური აღჭურვილობა განთავსებულია დაცულ ოთახშ(ებ)ი, სადაც დაიშვებიან მხოლოდ შესაბამისი უფლებამოსილების მქონე პირები;

ბ)ჩანაწერებზე წვდომა მინიჭებული აქვს დასაქმებულ პირთა მხოლოდ განსაზღვრულ წრეს, რომელთა წვდომის დონის და ფარგლების განსაზღვრისას მხედველობაში მიიღება თანამშრომელთა ფუნქციები და ჩანაწერებზე მათი წვდომის სამსახურებრივი საჭიროება;

გ)მიღებულია შესაბამისი ზომები სისტემის ინფორმაციული უსაფრთხოებისთვის, ინტერნეტიდან და კომპიუტერული ქსელიდან უკანონო შეღწევის პრევენციის მიზნით;

დ)სრულად აღირიცხება მონიტორინგის სისტემებში არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედება;

ე)აღირიცხება ჩანაწერების გამჟღავნების ყველა შემთხვევა.

12.5 შენახულ ვიდეოჩანაწერებზე წვდომა, მათი დათვალიერება და რიგ შემთხვევებში, მესამე პირებისთვის გადაცემა შესაძლოა, საჭირო გახდეს სხვადასხვა მიზეზით, მაგალითად, თუ არსებობს ეჭვი, რომ ვიდეოჩანაწერზე ასახულია დანაშაულის ან სხვა სამართალდარღვევის (მათ შორის ადმინისტრაციული სამართალდარღვევის) ფაქტი, შესაბამის ჩანაწერზე წვდომის ინტერესი უჩნდება საქმის მწარმოებელ ორგანოს

სისხლის სამართლის საქმის გამოძიებისა და ადმინისტრაციული სამართალდარღვევის საქმისწარმოების მიზნებისთვის.
12.6 ჩანაწერების დათვალიერებასა და მესამე პირ(ებ)ისთვის (მათ შორის, სამართალდამცავი ორგანოსთვის) გამჟღავნება ხორციელდება მხოლოდ კანონმდებლობით გათვალისწინებული შესაბამისი სამართლებრივი საფუძვლ(ებ)ის არსებობის შემთხვევაში.
12.7 სატელეფონო კომუნიკაციისას ზარების ჩანაწერების სისტემის (აუდიომონიტორინგი) მეშვეობით ავტომატურად ხორციელდება ცხელ ხაზზე, ასევე, ცხელი ხაზის მეშვეობით შესაბამის შიდა ნომერზე (ასეთის არსებობის შემთხვევაში) შემავალი ან აღნიშნული ნომრ(ებ)იდან გამავალი ზარების ჩაწერა და დამუშავება მომსახურების სრულყოფისა და ჯეროვნად შესრულების, განცხადებების, პრეტენზიების განხილვისა და რეაგირების, ეთიკის კოდექსისა და პროფესიული ქცევის სტანდარტების დაცვის მონიტორინგის, ასევე სხვა ლეგიტიმური ინტერესების დაცვის (მათ შორის, იურიდიული ძალის მქონე მტკიცებულების შექმნა) მიზნებისათვის, ან კანონმდებლობით პირდაპირ გათვალისწინებულ სხვა შემთხვევებში, ასევე, სადაც საჭიროა თანხმობის საფუძველზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი მოთხოვნების დაცვა.
12.6 აუდიოკონტროლის განხორციელება დასაშვებია მხოლოდ პირდაპირ „პერსონალურ მონაცემთა დაცვის“ საქართველოს კანონით გათვალისწინებულ შემთვევებში და სუბიექტის თანხმობის შემთხვევაში.

13. პერსონალური მონაცემების მესამე პირებისთვის გადაცემა

13.1 კომპანიამ მონაცემთა სუბიექტის პერსონალური მონაცემები შესაძლოა მესამე პირებს გადასცეს შემდეგი მიზნებისათვის: მონაცემთა სუბიექტის სრულყოფილი მომსახურებისთვის, საქართველოს კანონმდებლობით განსაზღვრულ შემთხვევებში, საქართველოს კანონმდებლობით კომპანიისთვის დაკისრებული მოვალეობების შესრულების მიზნით, ასევე სხვა მესამე პირებთან, სახელმწიფო სექტორში მოქმედ ორგანიზაციებთან გაფორმებული ხელშეკრულებებიდან გამომდინარე კომპანიის მიერ ნაკისრი ვალდებულებების შესრულების მიზნებისათვის.
13.2 მესამე პირს წარმოადგენს კომპანიის პარტნიორი ფიზიკური და/ან იურიდიული პირები, სახელმწიფო სექტორში მოქმედი ორგანიზაციები, რომელთან ურთიერთობის და ინფორმაციის გაზიარების აუცილებლობა გამომდინარეობს საქართველოს კანონმდებლობით და/ან სახელშეკრულებლო ურთიერთობიდან გამომდინარე ვალდებულებებიდან.

14. პერსონალური მონაცემების მესამე პირებისგან მოპოვება

14.1. კომპანიამ მონაცემთა სუბიექტის პერსონალური მონაცემები შესაძლოა მესამე პირებისგან მოიპოვოს შემდეგი მიზნებისათვის: მონაცემთა სუბიექტის სრულყოფილი მომსახურების მიწოდებისთვის, საქართველოს კანონმდებლობით განსაზღვრულ შემთხვევებში, საქართველოს კანონმდებლობით კომპანიაზე დაკისრებული მოვალეობების შესრულების მიზნით, ასევე მესამე პირებისგან, სახელმწიფო სექტორში მოქმედ ორგანიზაციებთან, პარტნიორ ორგანიზაციებთან გაფორმებული ხელშეკრულებებიდან გამომდინარე კომპანიის მიერ ნაკისრი ვალდებულებების შესრულების მიზნებისათვის.
14.2. მესამე პირს წარმოადგენს კომპანიის პარტნიორი ფიზიკური და/ან იურიდიული პირები, სახელმწიფო სექტორში მოქმედი ორგანიზაციები.

15. მონაცემთა უსაფრთხოება

15.1 კომპანიაში მიღებულია ისეთი გონივრული ორგანიზაციული და ტექნიკური ზომები, რაც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისგან, შეცვლისაგან, გამჟღავნებისგან, მოპოვებისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.
15.2 კომპანიაში მკაცრად არის დაცული პერსონალური მონაცემების კონფიდენციალურობა. მათზე წვდომა აქვთ მხოლოდ იმ თანამშრომლებს, ვისაც მონაცემების დამუშავება სჭირდებათ მათზე დაკისრებული მოვალეობების შესასრულებლად.
15.3. სტომატოლოგიურ კლინიკების ქსელ „დენსი“-ს ვებ-გვერდმა შეიძლება გამოიყენოს Cookies და/ან სხვა ტექნოლოგიები მონაცემთა შეგროვებისთვის, რეგისტრაციის პროცესის გასამარტივებლად და ვებსაიტის

ფუნქციონირებისთვის. Cookies არის მცირე ზომის ტექსტური ფაილები, რომლებსაც ვებ გვერდი ინახავს მონაცემთა სუბიექტის კუთვნილ ელექტრონულ მოწყობილობაში.

16. ელ-ფოსტისა და ტელეფონის ნომრის გამოყენების წესი.

16.1. ეფექტური და სწრაფი კომუნიკაციის მიზნით, კომპანია ამუშავებს დასაქმებული პირების, პერსონალის, თანაშემწეების, სტაჟიორების, მომსახურე პირების, ელ-ფოსტასა და ტელეფონის ნომრებს;
16.2. ელ-ფოსტისა და ტელეფონის ნომრის გამოყენება სიახლეების მიწოდებისა და სარეკლამო შეტყობინებების (პირდაპირი მარკეტინგი) გაგზავნის მიზნით დასაშვებია მხოლოდ სუბიექტის თანხმობით ;
16.3. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს ელ-ფოსტის ან/და ტელეფონის ნომრის გამოყენების შეწყვეტა მარკეტინგული მიზნებისთვის, რაც დაუყოვნებლივ უნდა დაკმაყოფილდეს.

17. მონაცემთა სუბიექტის უფლებები და ვალდებულებები

17.1 მონაცემთა სუბიექტს უფლება აქვს მოსთხოვოს კომპანიას ინფორმაცია მის შესახებ მონაცემთა დამუშავების თაობაზე. ასეთ დროს კომპანია მოთხოვნის თაობაზე შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) კალენდარული დღისა უზრუნველყოფს შემდეგი ინფორმაციის მიწოდებას:
17.1.1 რომელი კატეგორიის მონაცემები მუშავდება მის შესახებ;
17.1.2 რა მიზნით მუშავდება მონაცემები;
17.1.3 რა საფუძვლით მუშავდება მონაცემები;
17.1.4 რა გზით შეგროვდა პერსონალური მონაცემები;
17.1.5 გაცემულა თუ არა მისი მონაცემები მესამე პირზე, ვისზე გაიცა - მონაცემთა გაცემის საფუძველი და მიზანი.
17.2 მონაცემთა სუბიექტი უფლებამოსილია ნებისმიერ დროს მიმართოს კომპანიას და იმ შემთხვევაში, თუ მონაცემები არასრულია, არაზუსტია, არ არის განახლებული ან თუ მათი შეგროვება და დამუშავება განხორციელდა კანონის საწინააღმდეგოდ, მოსთხოვოს მისი პერსონალური მონაცემების გასწორება, დაბლოკვა, განახლება, დამატება, წაშლა, ან განადგურება. ასეთ დროს კომპანია შესაბამის რეაგირებას ახდენს შეტყობინების მიღებიდან არაუგვიანეს 15 (თხუთმეტი) კალენდარული დღის ვადაში.
17.3 მონაცემთა სუბიექტი უფლებამოსილია ნებისმიერ დროს, ყოველგვარი განმარტების გარეშე, გამოიხმოს (მოითხოვოს მონაცემების დამუშავების შეწყვეტა ან/და დამუშავებული მონაცემების განადგურება) მის მიერ კომპანიისთვის გაცხადებული თანხმობა მისი პერსონალური მონაცემების დამუშავების თაობაზე. იმ შემთხვევაში, თუ კომპანია პერსონალურ მონაცემებს ამუშავებდა მხოლოდ მონაცემთა სუბიქტის მიერ გამოხატული თანხმობის საფუძველზე, კომპანია უზრუნველყოფს შესაბამისი ქმედების განხორციელებას ასეთი შეტყობინების მიღებიდან არაუგვიანეს 5 (ხუთი) კალენდარული დღის ვადაში.

18. პერსონალურ მონაცემთა დაცვის ოფიცერი

18.1. კომპანიას ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების პროცესების შესაბამისობას პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან. საკუთარ საქმიანობაში დამოუკიდებელია და ექვემდებარება ცენტრის მმართველობის უმაღლეს რგოლს.
18.2. პერსონალურ მონაცემთა დაცვის ოფიცერი:
18.2.1. აკონტროლებს კომპანიაშ პერსონალურ მონაცემთა დამუშავების პროცესს;
18.2.2. საჭიროების შემთხვევაში მონაწილეობს მონაცემთა დამუშავების რისკების შეფასების პროცესში;
18.2.3. საჭიროების შემთხვევაში თანამშრომლობს პერსონალურ მონაცემთა დაცვის სამსახურთან;
18.2.4. უზრუნველყოფს თანამშრომელთა ინფორმირებასა და გადამზადებას პერსონალურ მონაცემთა დაცვის საკითხებზე;
18.2.5. განიხილავს მონაცემთა სუბიექტის განცხადებებს, საჩივრებს და/ან მომართვებს;
18.2.6. პერსონალურ მონაცემთა დაცვის საკითხზე შესაბამის დაინტერესებულ პირებს;
18.2.7. გამოავლენს, შეისწავლის და სათანადო რეაგირებას ახდენს პერსონალურ მონაცემთა დარღვევის ფაქტებზე.

19. პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი

19.1. სუბიექტის უფლებების ეფექტური დაცვისა და პერსონალურ მონაცემთა დაცვის კანონმდებლობის მოთხოვნათა ეფექტური შესრულების მიზნით, კომპანიაში განსაზღვრულია პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი - მენეჯერი.

19.2 კომპანიის დასაქმებულებს წვდომა აქვთ მხოლოდ იმ მონაცემებზე და იმ ფარგლებში, რაც აუცილებელია მათი მოვალეობების შესასრულებლად. თანამშრომლის შვებულების ან სხვა მიზეზით მოვალეობის შესრულების შეუძლებლობის შემთხვევაში მოვალეობის შემსრულებელს აქვს წვდომა ასევე იმ პირის წვდომის ფარგლებში, ვის მოვალეობასაც ასრულებს.

20. მონაცემთა საერთაშორისო გადაცემის წესი

20.1. კომპანია საქმიანობის მიზნებიდან გამომდინარე და შესაბამისი საფუძვლების გათვალისწინებით, დამუშავებული მონაცემები შესაძლებელია გადაიცეს საერთაშორისო ორგანიზაციისთვის ან/და სხვა სახელმწიფოში მყოფ/დაფუძნებულ პირთან, მათ შორის, კერძო ან საჯარო ორგანიზაციებთან. მონაცემთა გადაცემა ხორციელდება მხოლოდ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული წესითა და პროცედურებით.

21. პერსონალური მონაცემების შენახვა და განადგურება

21.1. კომპანია ინახავს მხოლოდ იმ პერსონალურ მონაცემებს, რომლებიც მას ესაჭიროება საქართველოს კანონმდებლობით დაწესებული ვალდებულებების შესასრულებლად მას შემდეგ, რაც პერსონალური მონაცემები აღარ ემსახურება ზემოხსენებულ მიზნებს, ისინი წაიშლება, განადგურდება ან სამუდამოდ ანონიმური გახდება .

22. დასკვნითი დებულებები

22.1 პასუხისმგებლობა პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით გათვალისწინებული წესების დარღვევისათვის განისაზღვრება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული წესების შესაბამისად.

22.2 კომპანიაში დასაქმებული პირები ვალდებულნი არიან დაიცვან დაწესებულების პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტი.

23. საკონტაქტო ინფორმაცია

შეზღუდული პასუხისმგებლობის საზოგადოება “დენსი” [საიდენტიფიკაციო ნომერი: **216335829**, იურიდიული მისამართი: საქართველო, ქალაქი რუსთავი, კოსტავას გამზირი, №11], კომპანიის მიერ პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე შეგიძლიათ დაგვიკავშირდეთ შემდეგ ელექტრონული ფოსტის მისამართზე: info@dens.ge ან/და კომპანიის ცხელი ხაზის ნომერზე: **032 2 599599**