Colosseum Dental Group

Group Data Protection Policy

Version 1.0/April 2019

Content

1. Purpose and Scope

This Group Data Protection Policy (the "**Policy**") is part of the compliance program of the Colosseum Dental Group (the "**Group**", also "**we**" or "**our**") and shall ensure that our Group-wide data processing complies with applicable data protection laws. As our Group processes sensitive personal data from our patients, ensuring appropriate data protection is key to maintaining patient trust and becoming the dental service provider of choice. This Policy lays down generally accepted data privacy principles without replacing European or national legislation. If European and/or national legislation foresees stricter requirements than what is stated in this Policy, the respective European and/or national legislation will take precedence over this Policy.

This Policy applies to all companies of the Colosseum Dental Group and our directors, managers, employees and healthcare professionals providing services to any of our Group companies (the "**Employees**") as well as our contractors and other contracting partners. All the above mentioned are expected to familiarize themselves with this Policy and all additional local policies and guidelines and to adhere to the principles set out therein when processing personal data.

Personal data in the meaning of this Policy is any information relating to an identified or identifiable individual (the "**Data Subject**"). Examples of personal data are name, (e-mail) address, phone number, bank details, date of birth, social security number, performance reviews or payroll information. As we are dealing with patients, we are mainly processing *sensitive* personal data, i.e. data relating to an individual's health. Such sensitive personal data is considered a special category of personal data and most applicable data protection laws require special protection for such sensitive personal data. In addition, information concerning our Employees may also contain sensitive personal data and needs to be protected and processed accordingly.

Processing in the meaning of this Policy means any action or operation performed with personal data, such as collection, storage, use, deletion, organization, alteration or disclosure of personal data. Examples of processing activities in our daily practice are making an appointment with a patient, entering patient information in our patient management system, accessing patient data from the patient management system upon a consultation, sending patient data to a supplier (such as a dental laboratory) for personalized products or sending invoices to patients. But also entering employee data in HR systems or collecting supplier contact details are processing activities. The term "processing" is very broad and Employees should assume that *any* operation relating to personal data of individuals is captured by and subject to this Policy.

2. General Principles for Collecting and Processing Personal Data

When processing personal data, certain general principles need to be respected. These principles can be found in the General Data Protection Regulation and most national data protection laws and they constitute the guiding principles for every data processing. The Colosseum Dental Group is committed to respecting these principles at all times when processing personal data.

2.1 Principle of Fairness and Lawfulness

Personal data must at all times be collected and processed in a fair and legal manner. This means that personal data may only be processed (i) if it has been obtained lawfully and (ii) in a way that takes into account the interests of the Data Subject. Please refer to Section 3 of this Policy to see when the processing of personal data is legally permitted.

2.2 Principle of Restriction to a Specific Purpose

Personal data may only be processed for the specific purpose that has been defined in advance and communicated to the Data Subject when his/her personal data was collected. The collected personal data must be relevant and limited to what is necessary for the purposes of processing. The use of personal data for a different purpose to the specific purpose for which it was collected is only possible to a limited extent. As a general rule, the purpose of the processing of personal data may only be changed to one that is compatible with the original purpose. The local Data Protection Officer shall be consulted in advance to find out if existing personal data may be used for other purposes. The purposes of processing must be defined in our internal documentation. When planning a new processing activity, please contact the local Data Protection Officer for assistance.

The personal data that we collect from our patients may generally only be used for providing dental services to our patients, unless the local law allows for further uses. In addition, such data may also be used for marketing purposes if local law allows and the patient's consent – if necessary – has been obtained. The Colosseum Dental Group does not tolerate the use of any patient data for any other purpose than that outlined in the informed consent form or the patient privacy notices. In particular, we do not tolerate the use of patient data for personal purposes by any Employee. In addition, in most countries where we operate, the national legislation provides for an obligation of medical secrecy for all medical and administrative personnel. The misuse of patient data will, therefore, also constitute a breach of this obligation and can even be a criminal offence.

Likewise, personal data about our Employees may only be collected and processed in connection with and in relation to the employment relationship and may not be processed for any personal use. For more information on how our Group processes personal data of our Employees, please refer to the local privacy notices for Employees.

2.3 Principle of Transparency

The principle of transparency requires that the Data Subject must be informed of what and how his or her personal data is collected and processed. In particular, the Data Subject must be informed about (i) the identity of the Colosseum Dental Group company that is responsible for the collection and processing of the personal data, (ii) the purpose(s) for which the personal data is processed (please refer to Section 2.2 of this Policy), (iii) the legal basis for the processing of personal data (please refer to Section 3 of this Policy), (iv) the categories of personal data that are processed, (v) the sources from which the personal data is collected, (vi) the recipients to whom personal data may be disclosed, (vii) the rights of the Data Subject (please refer to Section 7 of this Policy), and (viii) any other information to ensure fair and transparent processing of the personal data.

The appropriate way to inform the Data Subject about the above-mentioned points depends upon the circumstances. With respect to our patients, we inform them about these points in our informed consent form or the patient privacy notices available at our clinics and on the websites of the local Group company upon the making of an appointment or at the latest upon their first visit to our clinic. In case of updates, any changes to the patient privacy notices shall be communicated to our patients. When we enter into contracts, we ensure that our partners are informed about these points if the performance of the contract requires the processing of personal data. In addition, all our websites contain privacy notices explaining how we process the personal data of our patients, partners and job applicants within the Colosseum Dental Group. Furthermore, privacy notices explaining how we process the personal data of our Employees shall be available on the intranet of the local Group company. The local Data Protection Officer is responsible for ensuring that the Data Subjects are

informed of the processing activities of the respective Colosseum Dental Group company in accordance with the national laws.

2.4 Principle of Data Minimization

The personal data that is collected and processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. In other words, we may only collect those personal data that are relevant and necessary for the purpose(s) for which we want to process the personal data. Before collecting and processing any personal data, it must be verified if the envisaged processing method is the method that least infringes the privacy of the Data Subject(s) or whether there are other less invasive ways of processing the personal data to achieve the intended purpose.

The principle of data minimization also has an influence on how long personal data may be retained and stored. If the personal data is no longer necessary to achieve the purpose for which the personal data was collected, the data must be deleted, unless applicable laws provide for a longer retention period. Most national laws contain specific regulations on the retention of patient data and our Group must follow these regulations. In addition, if the Data Subject behind the personal data no longer needs to be identifiable but the data is still relevant for our Group, the personal data needs to be anonymized. For anonymization, please contact the local Data Protection Officer for assistance.

When planning the collection of personal data, we will determine and document retention periods for the collected data or, if we cannot determine specific retention periods, criteria according to which the retention period is determined.

2.5 Principle of Confidentiality and Data Security

The principle of confidentiality and data security requires that access to personal data may only be granted on a need-to-know basis. This means that Employees may access personal data only to the extent such access is necessary for them to fulfill their functions or duties.

Personal data must be treated as confidential at all times. Any unauthorized use or misuse of personal data is strictly prohibited. Employees may not use any personal data that they obtained in their professional function for private purposes. As mentioned above, national laws normally provide for an obligation of medical secrecy for all medical and administrative personnel. The misuse of patient data constitutes a breach of this obligation and can even be a criminal offence.

Personal data must be protected by adequate organizational and technical security measures. These security measures must ensure that personal data is protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. Please refer also to Section 4 of this Policy.

2.6 Principle of Accuracy

The personal data that we process must be correct, accurate and up to date. We shall not process erroneous or outdated personal data. We must take suitable steps to ensure that inaccurate, outdated or incomplete personal data in our systems is corrected, updated or deleted without undue delay.

2.7 Principle of Accountability

The measures related to the processing of personal data and the related risks must be regularly reviewed in order to ensure that the measures taken are sufficient to safeguard data protection and, where necessary, such measures shall be updated. Further, we will ensure that the data protection documentation is appropriate and up to date so that, for example, in case of an inspection by a national data protection authority, the compliance with data protection obligations in our Group's operations can be demonstrated.

3. Legal Basis for Processing Personal Data

All our processing of personal data must have a legal basis. A legal basis can, for example, be (i) the consent given by the Data Subject for the processing of his or her personal data, (ii) the performance of a contract such as the provision of healthcare treatment to our patients, (iii) a legal obligation of a Colosseum Dental Group company, or (iv) legitimate interests of a Colosseum Dental Group company.

The collection and processing of the medical data of our patients will normally be based on the performance of a contract and for carrying out our legal obligations.

The consent given by the patient, or any other Data Subject in connection with our processing activities, must always be documented. In case of a withdrawal of the consent, it must be ensured that any future data processing is stopped to the extent that the processing of the personal data was based on the consent given by the Data Subject.

The legal bases for each processing activity at our Group must be defined in our internal documentation. When planning a new processing activity, please contact the local Data Protection Officer for assistance.

4. Data Security

When processing personal data, we must implement appropriate technical and organizational measures (such as password protection, encryption, access control, non-disclosure commitments, physical access restrictions, etc.) to ensure a level of protection appropriate to the risk of our processing activities for the privacy of the Data Subject. The Colosseum Dental Group's IT department is responsible for defining the appropriate technical and organizational measures so that all the personal data processed within our Group is adequately protected.

All our Employees are responsible for securing their portable electronic storage devices as well as their laptops, mobile phones and physical and electronic files from unauthorized access.

5. Processing of Personal Data by Third Parties

The Colosseum Dental Group may also engage service providers that assist us in the processing of personal data. Examples of such service providers are the hosting provider that hosts our servers or the service provider that takes care of our payroll. Also, other companies of the Colosseum Dental Group that provide centralized administrative services for the whole Group are regarded as service providers for these purposes. Such service providers – also called data processors – may only process

the personal data according to our instructions. The respective Colosseum Dental Group company as the data controller always remains responsible for the correct processing of the personal data. Since the primary responsibility when outsourcing certain data processing activities remains with the outsourcing Colosseum Dental Group company, the agreement with the service provider must contain provisions concerning the extent of the assignment and the requirements concerning data protection and adequate data security. The service provider shall not have the right to process the personal data for its own purposes or connect the personal data with its own data registers. The service provider may only process the personal data to the extent required by the assignment and only in accordance with our instructions.

The local Data Protection Officer is responsible for ensuring that agreements with service providers contain the necessary clauses to protect the personal data that the service provider processes on behalf of the respective Colosseum Dental Group company.

6. Transfer of Personal Data to another Country

Some business activities of our Group might require that we transfer personal data to a party located in another country. For instance, the storing of personal data in a server in another country is considered an international data transfer. If that party is located in a country that fails to provide a legal framework regulating adequate protection for personal data, such data transfer will only be allowed if additional safeguards are taken to protect the personal data. As a general rule, personal data may not be transferred outside of the EU/EEA or Switzerland without the prior consent of the local Data Protection Officer. Please note that other companies of our Group are also considered to be third parties and additional safeguards must be implemented if a Group company receiving personal data is located in a country that does not provide for an adequate level of data protection.

The local Data Protection Officer shall ensure that adequate data protection safeguards are in place if personal data is transferred to a country outside the EU/EEA/Switzerland. If personal data is intended to be transferred to a country outside the EU/EEA/Switzerland, such fact shall be communicated to the Data Subjects.

7. Rights of Data Subjects

National and European data protection laws give the Data Subjects several rights so that they can control the processing of their personal data. For example, a Data Subject has the right to (i) be informed of the collection and processing of his or her personal data (please see Section 2.3 of this Policy), (ii) obtain confirmation as to whether or not personal data concerning him or her is being processed and, if data concerning the Data Subject is being processed, request a copy of the personal data being processed, (iii) request the respective company of the Colosseum Dental Group to rectify any inaccurate personal data, (iv) in certain cases, request the respective Group company to erase all personal data concerning him or her, (v) request the respective Group company to restrict the processing of personal data concerning him or her, and (vi) object to the processing of his or her personal data.

As part of our commitment to ensure a high level of data protection, the Colosseum Dental Group aims to respond to Data Subjects' requests concerning the exercise of their rights as quickly and effectively as possible. The local Data Protection Officer can be consulted in cases of complex access requests. Requests from Data Subjects must be fulfilled within **one month**. Only in cases of complex requests can the deadline be extended to a total of three months. But even if the deadline can be extended, the

Data Subject must be informed of such an extension within one month. Please remember that the identity of the Data Subject exercising his or her data protection rights must be confirmed before fulfilling the request made by the Data Subject. For further information on how to handle requests from Data Subjects, please refer to the local policies or guidelines relating to the Data Subjects' rights.

8. Data Processing Record

Each company of the Colosseum Dental Group that processes personal data must maintain a record of the processing activities under its responsibility. Each local Data Protection Officer is responsible for ensuring that his or her company maintains such a record for all processing activities under its responsibility in the respective country.

9. Data Protection Impact Assessment

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of the Data Subject, the respective company of the Colosseum Dental Group shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (so-called data protection impact assessment). The department or function that wants to set up the envisaged processing is responsible for performing the data protection impact assessment. The local Data Protection Officer assists the responsible department or function in performing this assessment. In any case, the Group General Counsel must be informed of any such assessment and its outcome.

Where the data protection impact assessment shows that the envisaged processing would result in a high risk for the Data Subject and the controller is unable to introduce security measures and safeguards to lower the risk, the national data protection authority must be consulted by the local Data Protection Officer. The consultation must be conducted before beginning to process personal data. Any such information of the national data protection authority shall be communicated to the Group General Counsel.

10. Data Breaches and their Notification

A personal data breach is a breach of security in our Group's systems (electronic as well as non-electronic) or processes that leads to an accidental or unlawful loss, destruction, alteration or unauthorized disclose of, or access to, the personal data processed by us. Data breaches not only include an attack by hackers but also the loss of data (for instance, a computer or a USB memory stick containing personal data being lost or stolen), the transfer of personal data to the wrong recipient(s) and any other incident that affects the confidentiality and integrity of the personal data we process (such as malware infection leading to data corruption).

If a (suspected) data breach is detected, it is important that immediate action is taken. In case of a personal data breach, the affected company of the Colosseum Dental Group shall notify the personal data breach to the national data protection authority without undue delay and **not later than 72 hours** after having become aware of it.

The local Data Protection Officer of the respective company of the Colosseum Dental Group needs to be informed immediately of a personal data breach. The Group General Counsel shall be informed of any major data breach. For more information on how to react in case of a data breach, please refer to the local policy or guideline relating to data breaches.

11. Data Protection Training

In order to foster a culture of data protection compliance, every company of the Colosseum Dental Group must implement data protection training for its Employees. The local Data Protection Officer is responsible for organizing and documenting this training.

12. Breaches of this Policy

It is the responsibility of each and every Employee of the Colosseum Dental Group to familiarize himself/herself with this Policy, the applicable local policies and guidelines and the requirements for data processing contained therein. We expect everyone working for our Group to adhere to the requirements stated in this Policy. Breaches of this Policy may lead to disciplinary action, ranging from a reprimand up to immediate termination of the employment relationship for repeated or very severe breaches. The specific disciplinary action for a certain breach will depend upon the severity of the breach and the Employee's behavior in rectifying such breach.

13. Assistance in Case of Questions

If you have any questions about this Policy or the correct way of processing personal data in a specific situation, you can always approach the local Data Protection Officer and ask for help.

14. Approval and Entry into Force

This Group Data Privacy Policy was approved by the Executive Committee of the Colosseum Dental Group on 9 April 2019 and entered into force on 1 May 2019.