DATA PRIVACY STATEMENT April 18, 2018

1.Introduction

This is the first data privacy statement of Medipol Ltd. (later referred to as "City Clinic") prepared in April 2018, prior to the entry into force of the European Union's General Data Protection Regulation ("GDPR"). The purpose of the statement is to demonstrate that City Clinic complies with the general data protection principles applicable in 2018. Compliance with data processing regulations has always been particularly important for a company operating in the field of aesthetic medicine and plastic surgery, as confidential and confidential information is handled in the industry.

Patient information at City Clinic is processed in the Skalpell patient information system and the Visia information system. The law defines general requirements for information systems and their manufacturers. The Skalpell patient information system is classified as a medical device (Class 1) in the European Union, and the manufacturer of the information system, Metodika, is responsible for demonstrating compliance with the system's requirements. Canfield and the Finnish importer of the system, Melon Ltd., are responsible for demonstrating the compliance of the Visia system.

Customers contact City Clinic by phone, email, and through contact forms on the website. A data protection agreement has been made with Applari Ltd., the maintainer of the website, regarding contact requests received through SSL-secured websites.

Contact requests are kept for one year unless the request leads to a customer relationship. Some procedures are sold in City Clinic's SSL-secured online store. City Clinic's website is SSL-secured. A data protection agreement has been made with MyCashflow, a Finnish service provider acting as a data processor.

Secure communication is also used in email correspondence at City Clinic. A secure site can be identified by a lock icon next to the browser's address bar and an https:// address.

City Clinic primarily collects information for the planning, implementation, monitoring, and billing of patients/customers' treatments. With the expansion of business operations, information has also been collected for the implementation of collaboration projects. In addition, information is collected for customer service, business development, and communication needs. A register containing information about City Clinic's professional staff is used for personnel matters.

2. New legislation

The EU General Data Protection Regulation, adopted in the EU, will apply from May 25, 2018. The aim of the regulation is to establish a uniform data protection regulation for EU citizens. This data privacy statement assesses the requirements of the upcoming data protection regulation for the processing of personal data by City Clinic.
For City Clinic's operations, the new regulation does not require extensive measures as the industry is already governed by clear laws. The rights and position of patients are precisely defined in the law. Legislation regarding the handling, management, and retention of patient records, among other things, already has a broader impact on City Clinic's data processing than the upcoming data protection regulation. Therefore, the new regulation does not bring significant changes to City Clinic's operations.

The most significant change is the obligation for the data controller (City Clinic) to demonstrate compliance. City Clinic must be able to reliably demonstrate that the company operates in accordance with the regulation and other legislation. Another change is that the new regulation takes a risk-based approach: the risks associated with the processing of personal data must be assessed in advance before the processing begins.

Due to the processing of health data at City Clinic, a comprehensive risk-based impact assessment regarding data protection has been conducted. Most importantly, the company responsible for maintaining the patient information system has conducted a comprehensive risk-based impact assessment of the information system.

2.1 Obligation to Demonstrate Compliance

Compliance with the new regulation cannot be achieved solely by appropriately handling data. As of May 25, 2018, lawful processing of data must also be demonstrable. Processes related to the processing of personal data, as well as privacy measures, must be documented. The documents should indicate that the data is being processed in accordance with the law. Privacy measures should be transparent and systematic.

City Clinic demonstrates compliance with the law through various types of privacy notices. The most important privacy notice concerns the patient data registry.

2.2 Embedded and Default Privacy

Privacy must be an integral part of the processing of personal data. We talk about embedded privacy, which is a fundamental requirement for those operating in the healthcare sector.

New technologies and communication tools have brought new dimensions to privacy. Since an aesthetic medical clinic deals with patient data, new technologies and communication tools need to be carefully assessed. By default, personal data should always be processed in the most limited manner possible.

2.3 Reporting Security Breaches

According to the data protection regulation, a notification must be made within 72 hours of becoming aware of a personal data security breach. Since a breach of the data processed at Cityklinikka would pose a high risk to the rights of the data subjects, the affected individuals themselves must also be notified, even though patient data in Cityklinikka's patient information system is always encrypted.

Cityklinikka has established processes to handle security breaches. For patient information, most of the process planning comes directly from the administrator of the patient information system.

Security breaches targeting systems other than patient records are handled according to internally established guidelines. The crisis communication plan designed by the spokesperson forms the basis for actions in potential security breach situations.

3. Contracts with Data Processors

According to the new regulation, a data processor is a natural or legal person who processes personal data on behalf of the data controller (in this case, Cityklinikka). Cityklinikka has identified all data processors for each register. Written agreements regarding compliance with the data protection regulation have been or are being made with them.

In new collaboration, partnership, and subcontracting agreements, the requirements of the data protection regulation will be taken into account from the beginning.

4. Data Protection Officer

Cityklinikka is a small and medium-sized enterprise (SME) where the core activities do not involve processing of personal data. Therefore, the company has not appointed a Data Protection Officer. The responsibilities related to compliance with the data protection regulation have been distributed as follows:

- The company's management is responsible for ensuring compliance with the data protection regulation.
- The Patient Ombudsman serves as the contact person for individuals in the patient data register.
- The Communications Officer serves as the contact person for individuals in the digital communications register and other non-patient data registers.
- The Office Manager acts as the contact person for staff in matters related to data protection.
- The Communications Officer is responsible for keeping the company's top management and staff informed about the requirements of the data protection regulation.

5. Rights of Data Subjects

The data protection regulation introduces new rights and provides clarifications to existing rights concerning data subjects. The application and interpretation of these rights are not

entirely clear in all aspects. Cityklinikka, among others, is awaiting guidance from the EU's data protection group and future legal precedents.

5.1 Right to Information on the Processing of Personal Data

As the data controller, Cityklinikka has an obligation to provide transparent information about the processing of personal data. The information should be concise, easily understandable, and readily available. Privacy notices concerning the patient register and digital communication register of Cityklinikka have been drafted in clear Finnish language. These privacy notices can be found on Cityklinikka's website. Both can also be provided to the data subject in printed or electronic form. Other privacy notices will be provided to the data subject upon request. Requests can now also be made electronically. If necessary, Cityklinikka may ask the data subject for additional information to verify their identity. This ensures the realization of the data subject's rights without violating the rights of other data subjects.

A new matter to communicate is also the notification of the retention period for personal data.

5.2 The right to access information

Under the data protection regulation, individuals have the right to access their own information, also known as the right to access. In practice, this means that upon request, Cityklinikka must inform the individual whether their personal data is being processed by the company or not. The information must also be provided to the individual if requested. The access request can now be made electronically following the enactment of the new regulation. If necessary, Cityklinikka may request additional information from the individual to verify their identity. This ensures that the rights of other individuals are not infringed upon. According to the data protection regulation, the request from the individual must be responded to within one month.

5.3 The right to rectification of data

If a data subject finds incorrect personal data in their records, they have the right to request Cityklinikka to correct the inaccurate information. Information about the actions taken by the company to rectify the data must be provided to the data subject within one month of the request. The data protection regulation does not specify the procedures for rectifying the data.

5.4 The right of the data subject to be informed about a data breach

Cityklinikka has taken all possible measures to prevent data breaches and ensure data security. However, if a data breach were to occur, such as unauthorized disclosure of personal data to a third party, Cityklinikka would be obligated to notify the data subject about the incident.

5.5 The right to restrict processing

The data subject has the right to restrict the processing of their personal data, at least temporarily.

5.6 The right to be forgotten

Data from the patient register and employee register will be deleted if the data subject's request is justified. In such cases, the request should be sent in writing to the CEO of Cityklinikka. For other registers, the data subject has the explicit right to delete information concerning themselves.

5.7 The right to data portability

In certain situations, the data subject has the right to transfer their personal data to another data controller in a machine-readable format, if technically feasible. However, the right to data portability cannot be applied to the personal data registers of Cityklinikka, as it is not technically possible to transfer the data from one system to another.

5.6 The right to object to processing, automated decision-making, and profiling

An individual in the register has the right to prohibit the processing of any personal data concerning them, particularly when the data is used for marketing or research purposes.

6. Information and Risk Management

The information stored in City Clinic's records is consistent, as up-to-date as possible, and unambiguous.

During the risk analysis, the registers were classified into security levels, with security level 1 containing confidential information whose breach would pose a high risk to the rights of the registered individuals. Patient data belongs to security level 1. Only healthcare professionals and their assistants directly involved in the treatment are authorized to handle patient data. Those responsible for appointment scheduling have limited access to patient information. The spokesperson in charge of online sales handles customer purchases and not actual patient data. Patient data is not processed on social media platforms.

At City Clinic, patient data may only be handled to the extent required by the assigned tasks. All patient information is considered confidential. Staff members are required to sign a confidentiality agreement at the beginning of their employment.

All manual materials related to the registers are kept in lockable archives. Electronically stored information is protected by electronic access rights. Compliance with legal requirements ensures data security.

The users of the information, their access rights, and the devices used for data processing are defined for the patient information register. Patient data can only be processed using designated devices.

Risks related to information security are assessed semi-annually or more frequently if necessary. External (outsourced services) and internal (security meetings) monitoring is conducted to ensure information security.