Appendices for 3Shape Communicate

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:
The purpose of 3Shape Communicate and processing activities related to it is facilitated storage and sharing of the data that is uploaded by the data controller to 3Shape Communicate service.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
• Storage • Transfer • Deletion • Anonymisation • Analytics & Statistics

A.3. The processing includes the following types of personal data about data subjects:
Name, middle name, surname, scan of the upper and lower jaws, other relevant treatment data

A.4. Processing includes the following categories of data subject:
Patients of the data controller

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:
The data processor processes data on behalf of the data controller as long as the data controller has an active 3Shape Account used to log in to 3Shape Communicate, unless the data controller deletes the data (cases) from 3Shape Communicate earlier.

Appendix B Authorised sub-processors

B.1. Approved sub-processors
On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors: List of 3Shape's sub-processors - 3Shape The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing
The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following: • Ensuring the storage of data • Ensuring the transfer of the data to other actors • Ensuring deletion of data • Ensuring anonymisation of data • Enabling data analytics & statistics

C.2. Security of processing

The level of security shall take into account that the processing involves a large volume of personal data which are subject to Article 9 GDPR on 'special categories of personal data' which is why a 'high' level of security should be established. The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor hereby informs that the following security measures have been implemented:

Organizational security measures

Policies for information & personal data security

3Shape prioritizes the security and privacy of information and personal data. 3Shape has implemented comprehensive policies that govern how information and personal data is handled and protected to ensure that it is secure and processed in compliance with the highest industry standards and regulations, especially GDPR and HIPAA (including Information Security Policy, Data Protection Policy, Access control policy, Back-up Policy, Acceptable Use Policy, Retention Policy etc.)

Roles and responsibilities management

3Shape has implemented comprehensive roles and responsibilities management, which ensures that all roles related to the processing of information and personal data are clearly defined and assigned within our organization. This also includes the appointment of a Data Protection Officer (DPO) who plays a key role in ensuring that 3Shape complies with data protection laws and practices.

Risk Management

3Shape has implemented procedures that mandate regular risk assessments to identify and address any security vulnerabilities. Additionally, 3Shape assesses the risks of its activities on the privacy of data subjects when processing personal data.

Employee Training and Awareness Programs

3Shape prioritizes employee education and training in protecting information and personal data through mandatory regular trainings, various programs and campaigns to increase information security awareness.

Confidentiality of personnel and other people if having access to customer information and personal data

Shape ensures the confidentiality of all personnel and any other individuals who have access to customer information and personal data. Confidentiality clauses in employment contracts, separate NDA agreements, and security policies are in place to govern the handling of information and personal data.

Data Classification

Besides the measures already mentioned, a key requirement of the system design is to ensure high availability and robustness against malicious actions to gain access to data or deny users temporary access to their data.

Incident Response Plan (IRP)

3Shape has developed a comprehensive Incident Response Plan (IRP) to quickly and efficiently address any security incidents or data breaches. This plan outlines the steps which must be taken from the initial detection of an incident through to resolution and post-incident analysis. It ensures that 3Shape can contain threats, minimize damage, and recover operations with minimal disruption.

Disaster Recovery & Business Continuity Plans

3Shape maintains disaster recovery and business continuity plans and processes to ensure the continuation of services and effective recovery. These plans are regularly tested to ensure their accuracy and efficiency in the event of an emergency.

Change Management Procedures

3Shape has established procedures for managing changes to systems, software, and configurations. These protocols ensure that any modifications undergo thorough planning, documentation, review, and implementation.

Audit and Compliance Reviews

3Shape conducts regular audits and compliance reviews to ensure adherence to industry standards and regulatory requirements. These reviews involve thorough assessments of 3Shape's security measures, policies, and procedures to identify any gaps or non-compliance issues. Any findings are proactively communicated to data owners, and remedial measures are implemented promptly.

Third Party Management

3Shape manages third-party involvement by selecting and overseeing external partners and vendors who have access to our systems or handle personal data. 3Shape implements strict compliance review processes to assess third-party security practices and ensure they comply with 3Shape's standards and regulatory requirements.

Technical security measures

Access controls

Users in 3Shape Communicate are managed and authenticated through 3Shape Account, ensuring each user has a unique ID. This guarantees that dental professionals have access only to their own cases. Role-based access control allows different users to have access to specific resources based on their roles.

To prevent unauthorized access to patient information on unattended workstations or lost mobile devices, the 3Shape Communicate website and iOS application automatically log off after 15 minutes of inactivity. Authorization information and sessions also expire after 15 minutes.

Data Encryption

Data sent via 3Shape Communicate is encrypted. This ensures that even if the data is intercepted during transmission to 3Shape Communicate servers, it remains unreadable to unauthorized parties. 3Shape Communicate encryption type: TLS 1.3 AES_256 encryption.

Data protection techniques

Sensitive data in 3Shape Communicate is protected through tokenization or removal of sensitive details before access is granted to users with lower authentication protocols or to administrative-level users who do not own the data. This ensures that personal and sensitive information remains secure at all times.

Integrity controls

3Shape Communicate ensures data integrity and security at every step. Industry-standard algorithms prevent unauthorized tampering, ensuring data is received as intended. Users have full control to delete orders and patient information. Redundant file storage and the TLS 1.3 protocol protect against data loss and improper modifications during transmission. Digital signatures guarantee the validity of all authorization information.

Logging and Auditing

3Shape Communicate includes comprehensive logging mechanisms that record every instance of access to patient data. Logs are generated in situations such as when a customer care team member accesses personal health information to provide support, when a service technician performs maintenance activities involving such data, or when a customer accesses their own personal health information. These access logs are regularly audited to ensure that all access to patient data is appropriate and authorized, enhancing the security and privacy of the information.

Intrusion Detection and Prevention

3Shape Communicate employs advanced intrusion detection and prevention systems. Multi-layered access controls are utilized across all levels of the infrastructure to prevent unauthorized access. Leading intrusion detection technology is used to ensure continuous protection for storing sensitive information.

Firewalls

3Shape Communicate is protected by application-level firewalls that filter out unauthorized requests. Access to services, databases, and dependencies requires specific credentials, ensuring stringent security controls.

Secure Coding Practices

Security is integral to the development of 3Shape Communicate. Secure coding is prioritized from the start, with extra time dedicated to security improvements. Every code update is carefully reviewed by another developer to ensure it meets high security standards before testing and release. This thorough review process helps keep the software secure and reliable.

Patch Management

3Shape has adopted the ideology and techniques of CI/CD (continuous integration and continuous delivery). Tasks are prioritized and worked on daily, with results constantly pushed to a pre-production environment Once several features or bug fixes are present in pre-production, they are released. Releases typically occur once a week on average. However, urgent updates may be released out of schedule when necessary.

Backup and Recovery

All data storage in Communicate is continuously backed up using either locally-redundant or geo-redundant methods. This ensures protection against internal drive malfunctions and, with geo-redundancy, safeguards against regional service disruptions. Databases are backed up daily, allowing for recovery in the event of data loss. These backups are retained for 30 days to provide a safeguard against data corruption.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- A process for data subject request
- A process for data breach

In an event of a data breach, data processor will provide an analysis report of the event along with other available information that will be necessary to support the data controller's follow up action(s).

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall, upon request from the data controller, either delete, anonymise, or return the personal data in accordance with Clause 11.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorization.

Physical location of data stored by sub-processor:

Personal data of customers located in Europe (including their patients' data) is stored within European Union: Ireland (Microsoft Azure Cloud).

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor
The data processor shall on an annual basis, upon the request of the data controller, send a declaration of compliance with this Clauses to the data controller free of charge. The declaration type is to be defined by the data processor. Based on the results of such an inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The data controller or the data controller’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required and can argument the requirement. The data controller’s costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors
The data processor shall once a year obtain a proof of the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. Upon the data controller’s request, such a proof of compliance may be submitted to the data controller for information.

Appendix D The parties’ terms of agreement on other subjects

N/A