Technical and Organisational Security Measures

Rosa must implement appropriate security measures to protect the personal data it processes against unauthorized access, modification, or destruction.

Data security and confidentiality and patient privacy will comply with applicable laws, including the European General Data Protection Regulation (***GDPR***).

Furthermore, to ensure that you can fully trust us with the management of your information, Rosa is in the process of becoming ISO/IEC 27001 certified.

ISO is the “International Organization for Standardization”, an independent organization that develops international standards for security and safety. ISO 27001 is an information security standard that describes the best way of keeping information (including the information we collect about you, as described in this policy) secure. It requires businesses to have a world-class information security management system in place so that the data they handle is rigorously protected.

These Technical and Organisational Security Measures (***Security Measures***) explain how Rosa ensures the security of the personal data it processes. They describe the set of measures, procedures, and processes that Rosa has implemented to ensure the availability, integrity, and confidentiality of all forms of information, with the aim of ensuring the continuity of the information and the information provision, including the underlying IT infrastructure, and to limit the possible consequences of security incidents to an acceptable, predetermined level. “Rosa” is Rosa ASBL, a non-profit organization established at Cantersteen 10, 1000 Brussels, with enterprise number 0745.832.604.

If you have an agreement with Rosa as a health professional or as a registered patient, these Security Measures are part of that agreement.

To communicate with Rosa about these Security Measures, please send an email to security@rosa.be.

Technical Measures

Technical measures refer to the measures and controls that Rosa puts in place to its systems and any technological aspect of the organisation, including devices, networks and hardware.

Data Storage
All personal data and information processed by Rosa is stored in the cloud and not at a location owned or operated by Rosa. A copy of production data is stored locally on a Rosa owned device which is encrypted (at rest). Rosa’s cloud service provider(s) is responsible for

the security of its data centres. On a regular basis and at least once a year, Rosa performs due diligence of its cloud service provider(s), including obtaining and reviewing security compliance certifications.

Availability

Our infrastructure is configured to provide high availability. Rosa's databases and servers are deployed across multiple data centers. If one of the data centers is down, our services will remain available. Our applications are also hosted behind a Content Delivery Network. This provides extra caching and helps mitigate distributed denial of service (DDoS) attacks.

Environment segregation

Rosa ensures a strict separation between production and non-production environments to reduce the risks of unauthorised access or changes to the operational environment. The production environment is isolated in a dedicated network. Rosa's non-production environments are used for development, testing, and staging purposes. There is no testing with production data.

Cybersecurity

Rosa has implemented detection, prevention and recovery controls to protect its systems and data against malware (such as viruses, spyware and ransomware). Internet connection and Rosa's internal network are secured with a powerful firewall.The wifi network is password protected and guests are using a separate wifi network. To avoid modification or misuse of Rosa's assets, conflicting duties or responsibilities are carried out by different persons. When this is impossible to achieve, because of the limited size of Rosa, other measures (such as monitoring or supervision) are taken.

Encryption

Rosa uses encryption to protect confidential and sensitive information at rest and in transit.

Physical security

Rosa has implemented physical security controls that are appropriate to the level of risk posed by the information held and the nature of operations at Rosa's offices. Rosa's offices are located in a building with access restricted to holders of access cards provided upon a formal approval process. Rosa's offices and meeting rooms are restricted to personnel with a need to access those areas to carry out their job functions. Personnel access cards are revoked when they are no longer needed, including within 1 business day of the relevant personnel changing role or leaving Rosa. Hard copies of records are stored in a locked cabinet. Visitors are escorted in all non-public spaces and never left unattended. Fire alarms and extinguishers are checked at regular intervals and their access is not blocked.

Appropriate Disposal

Rosa ensures that paperwork and devices that contain or may contain personal data or other sensitive information are securely destroyed so that personal data or sensitive information cannot be retrieved by an unauthorised individual. All hard copies, credit cards and CD/DVD-roms that are no longer needed are shredded in the office. Hardware devices are securely wiped and stored in a secured location before being picked up by a nationally recognised hardware destruction company for recycling or destruction.

Passwords
Rosa requires internal and external personnel and systems and (cloud) services holding confidential or sensitive information to set strong passwords and, wherever available, to enable multi-factor authentication. Two Factor Authentication is required for systems holding sensitive and confidential information. Passwords are stored encrypted/hashed and separated from other data and login information is transmitted encrypted.

Access Rights
Access to databases containing personal data and access to documents containing sensitive data is only granted on a need-to-know/need-to-use basis. All staff having access to such databases or sensitive documents is bound by confidentiality and security obligations. Logical access lists are reviewed on a regular basis, depending on the classification of the information. User access rights are reviewed every quarter. Access to Rosa's systems is revoked within 1 business day of an employee or contractor leaving Rosa.
Rosa keeps a log of all accesses to its databases.

Organisational Measures

Organisational measures refer to the policies, standard of procedures, and audits that Rosa puts in place to ensure consistency in the protection of personal data during the full cycle of the processing.

Information Security Management System (ISMS)
ISMS refers to Rosa's written security framework of policies and procedures setting out the administrative, technical and physical safeguards designed to protect the personal data and other sensitive information held by, or on behalf of, Rosa. In other words, it describes Rosa's approach to information security and privacy. Rosa maintains a comprehensive ISMS that applies to all its stakeholders: all systems, people, and processes that constitute Rosa's information systems, including board members, employees, customers, suppliers, and other third parties who have access to Rosa systems. It aims at establishing effective safeguards for the information processed at Rosa, ensuring the continuity of the information and the information provision, including the underlying IT infrastructure, and limiting the possible consequences of security incidents to an acceptable, predetermined level. Rosa's ISMS is maintained by a dedicated security team, led by Rosa's Chief Security Officer. Rosa monitors compliance with its ISMS and conducts ongoing training of its staff to ensure compliance. The ISMS is reviewed and updated at least annually to reflect changes to the organisation, business practices, technology, services and applicable laws and regulations. Rosa will not amend the ISMS in a way that materially weakens or compromises the effectiveness of its security controls. As part of the ISMS, Rosa has developed and adopted a formal Information Security Policy that has been reviewed and approved by the top management of Rosa.

Business Continuity Policy and Disaster Recovery Plans
Rosa maintains a documented Business Continuity Policy and Disaster Recovery Plans. Our Policy and Plans include: (i) clearly defined roles and responsibilities; (ii) Recovery Point Objectives; (iii) Recovery Time Objectives and (iv) Backup policy. Rosa reviews and updates

its Business Continuity Policy and Disaster Recovery Plans at least annually. Backups are tested monthly.

Incident Management Process

Rosa has developed and maintains an Incident Management Process to be used in the event of an actual or suspected data breach or other security incident. It sets out clear roles and responsibilities, reporting mechanisms, and procedures for classifying, containing and recovering from the incident. It also includes procedures for required notifications to relevant authorities and affected individuals as well as mechanisms designed to prevent future similar incidents.

Software Development Process

Rosa's Software Development Process includes principles and rules around storage of source code, review of source code and rules and principles applied in the design and engineering of systems, networks and infrastructure. Network/system architecture and designs are always peer-reviewed and any change to Rosa's network/system architecture is first tested and released in Rosa's staging environment before being applied to the production environment. Security is designed to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

Penetration Testing and Risk Assessments

Rosa undergoes regular audits from both internal and external security teams. Internally, Rosa undergoes regular internal risk assessments under the responsibility of the Risk Manager. Rosa also regularly performs non-notified audits and phishing exercises targeting its staff. At least once every three years or after a major change to Rosa's architecture/infrastructure, Rosa is also subject to external penetration tests by a nationally recognised security firm.

External Data Protection Officer (DPO)

Rosa has appointed an external DPO reporting directly to the senior executive team and with experience in legal, in tech and in the health sector. Rosa's DPO is responsible for (i) informing and advising Rosa and its employees, of their obligations under data protection laws; (ii) liaising with the internal Privacy Officer on privacy-related matters; (iii) monitoring compliance of Rosa with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations; (iv) providing advice where a Data Protection Impact Assessment has been carried out and monitoring its performance; (v) acting as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights; and (vi) cooperating with Data Processing Authorities (DPAs) and acting as a contact point for DPAs on issues relating to data processing.

Training

All employees at Rosa and, where relevant, contractors, receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function. In addition to these mandatory trainings, Rosa offers its staff additional training resources, including additional security readings and hackathons.

Due diligence Checks
Rosa performs background checks on all new recruits as well as third-party contractors with access to Rosa’s systems and information. All employees and contractors are bound by confidentiality obligations that survive termination of their employment or collaboration agreement. Rosa maintains a formal disciplinary procedure for violation by its staff of their security and confidentiality obligations.

Other Policies and Procedures
Rosa has implemented additional policies and procedures to ensure that its information and assets are effectively protected. These include, amongst others, an information classification policy, an information retention policy, an access control policy, a cryptography policy, a password policy, a mobile device policy and a code of conduct covering additional security aspects, such as remote working, the usage of own devices and the use of electronic messaging and file sharing. Each policy is evaluated at least once a year.

Changes to the Security Measures

These Security Measures are current as of 14 January 2022. We keep this document under regular review to ensure it is current and we may edit it over time to reflect the changes in our services and data processing activities. If we do so, we will post the updated Security Measures on this webpage. Please refer back to these Security Measures to review any amendments as any revised Security Measures will apply to all personal data processed by Rosa.