Gottsegen György National Cardiovascular Center

Data Protection, Confidentiality and Information Security Notice

Any person carrying out activities at the Gottsegen György National Cardiovascular Center shall treat as confidential any personal data, special category data, health data, business secrets and any other non-public professional, financial, technical or organisational information that comes to their knowledge in connection with an existing or future legal relationship with the Institute, and shall use such data and information only to the extent necessary for the performance of their tasks, in accordance with applicable laws, instructions given by the Institute and internal regulations.

1. Subject matter and scope of the Notice

1.1. This Notice applies to all data and information that a person carrying out activities at the Institute becomes aware of, processes, records, transmits or otherwise accesses in connection with the establishment, existence or termination of their legal relationship, or during the performance of their tasks.

1.2. The scope of this Notice includes, in particular, patient data, staff data, health records, financial and human resources data, data related to IT systems, and non-public information concerning the operation of the Institute.

1.3. The confidentiality obligation set out in this Notice remains in force without time limitation after the termination of the legal relationship.

1.4. This Notice applies throughout the entire duration of the legal relationship of any person carrying out activities at the Institute. The confidentiality and data protection obligation remains in force without time limitation after the termination of the legal relationship.

2. Confidentiality and data processing obligations

2.1. A person carrying out activities at the Institute may access and process data only to the extent necessary for the performance of their tasks or for the activity carried out at the Institute, in accordance with the authorisations granted to them and the instructions issued by the Institute, and in compliance with the principles of necessity and proportionality.

2.2. The person may not make confidential data or information that come to their knowledge accessible to any unauthorised person, disclose them, transmit them, copy them, photograph them, export them, or use them for their own benefit or for the benefit of another person.

2.3. Documents containing personal or health data may be transmitted outside the Institute only for a lawful purpose, by authorised means and with the application of the necessary technical and organisational protective measures.

2.4. It is prohibited to save or transmit data to private devices, private e-mail addresses, unauthorised cloud services or unauthorised data carriers.

2.5. A person carrying out activities at the Institute must keep the identifiers and passwords provided to them confidential, may not disclose them to any other person, and may not use another person's access on behalf of someone else.

2.6. The confidentiality obligation does not affect statutory data provision and cooperation obligations towards authorities.

3. Work organisation and information security rules

3.1. A person carrying out activities at the Institute has the basic information security knowledge required for their activity and shall familiarise themselves with and comply with the applicable Information Security Policy in force at all times. The Policy is available on the GOKVI intranet at: https://gokvi.gokvi.local/mir/sz/sz.html

3.2. A person carrying out activities at the Institute shall use the Institute's information systems, applications and IT devices exclusively as intended, with the utmost care expected of them, and shall make every effort to ensure that the Institute's interests, data or systems are not harmed as a result of their intentional or negligent conduct.

3.3. A person carrying out activities at the Institute must comply with the "clean desk" and "clear screen" principles: when leaving the workstation, they must lock it or log out, keep confidential documents secured, and not make them accessible to unauthorised persons.

3.4. Printed documents or notes may be used only to the extent necessary for the performance of tasks; unnecessary copies must be destroyed or handed in in accordance with internal regulations.

3.5. In the case of remote access, home working or tasks performed at an external location, the same data protection and information security requirements apply as when work is performed on the premises of the Institute.

3.6. A person carrying out activities at the Institute must immediately report to the contact person designated by the Institute or, where applicable, to their direct superior, and to the organisational unit competent under the internal procedure, any event, suspicion or detected breach that indicates a data protection incident, unauthorised access, data loss, data leakage, breach of information security rules or any other security event.

4. Obligations related to termination of the legal relationship

4.1. Upon termination of the legal relationship, a person carrying out activities at the Institute must immediately return all documents, data carriers, devices, access cards and other information carriers owned or managed by the Institute.

4.2. Any copies, notes or electronic files containing confidential data relating to the Institute that are in their possession must be handed over, deleted or destroyed in accordance with the instructions of the Institute.

5. Final provisions

5.1. A breach of the obligations set out in this Notice constitutes a breach of obligations arising from the legal relationship and may result in legal consequences under the applicable laws.

5.2. This Notice is governed in particular by Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), Act LXIX of 2024, Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data, Act CLIV of 1997 on Health Care, Act C of 2020 on the Health Service Employment Relationship, Act I of 2012 on the Labour Code, Act LIV of 2018 on the Protection of Trade Secrets, and the Institute's internal regulations in force at all times, including in particular the Data Management and Data Protection Policy and the Information Security Policy.

5.3. This Notice forms part of the documentation relating to the legal relationship of the person carrying out activities at the Institute and to the activity performed at the Institute.