Personal data security policy



# Object of this document

The object of this Policy is to determine principles and rules of activities aimed at providing personal data processing security in MDH. The policy specifies authorisation process, handling of data in traditional form, as well as supervision over data processing and over processing documentation.

# Principles of personal data processing

* 1. MDH Sp. z o.o. acts as a controller of personal data subject to processing.
  2. Duties related with information security are specified in the Information Security Policy.
  3. Access to personal data is restricted to persons authorised to process them and only these persons can process discussed data.
  4. BUM issues an application to grant authorisation. Where necessary, in order to properly determine the scope of authorisation, he shall consult DPS. During employment procedure authorisation for a new employee shall be approved by the Management Board. Authorisations granted to IT systems are described in the IT system management instructions.
  5. All information concerning new employee must be submitted to DPS.
  6. When the authorisation is granted, new employee shall be entered into register of authorised persons, as specified in the template of annex 5 and according to information delivered by the employee, who prepares the authorisation, and ITSC.
  7. Change of the employment duties and related changes in the scope of authorisation require cancellation of the current authorisation and granting of the new one.
  8. In case of employment termination all authorisations shall automatically expire.
  9. Third parties can have access to personal data only under applicable provisions of law.
  10. If personal data is transferred for processing within the scope of activities performed by MDH, such transfer is governed by the personal data entrusting agreement.
  11. Confirmation or suspicion of person data security breach shall be immediately reported to BUM or directly presented to the Management Board, as specified in the Incident Management Procedure.
  12. Personal data processing shall be supervised on a regular basis by BUM and monitored by DPS.
  13. Useless printouts, i.e. including incorrect data and invalid documents, shall not be stored but shall be destroyed in dedicated shredders.
  14. All documents containing personal data shall be protected against access of third parties. Documents shall remain within the processing area.
  15. Following accomplishment of performed tasks documents must be stored in cabinets, drawers and archives with locks.
  16. BUM shall supervise, if personal data processing complies with the accepted security procedures and principles.

# Obligation to provide information

* 1. BUM shall be responsible to provide information to data subjects.
  2. Under Article13 of GDPR, at the time when personal data are obtained, specific information shall be provided to data subject.
  3. Discussed information shall cover:
     1. full name and contact details of the controller;
     2. the contact details of the data protection supervisor;
     3. the purposes of the processing for which the personal data are intended as well as the legal basis of the processing;
     4. the legitimate interests of processing;
     5. the receivers or categories of receivers of the personal data;
     6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation;
     7. the period for which the personal data will be stored, or the criteria used to determine that period;
     8. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
     9. where the processing is based on a consent - the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
     10. the right to lodge a complaint with the President of the Personal Data Protection Office;
     11. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
     12. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  4. Under Article 14 of GDPR, where personal data have not been obtained from the data subject, the following information must be provided:
     1. full name and contact details of the controller;
     2. the contact details of the data protection officer;
     3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
     4. the categories of personal data concerned;
     5. the receivers or categories of receivers of the personal data;
     6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation;
     7. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
     8. the legitimate interests of processing;
     9. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
     10. where the processing is based on a consent - the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
     11. the right to lodge a complaint with the President of the Personal Data Protection Office;
     12. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
     13. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  5. The information referred to in paragraph 3.4 (where personal data have not been obtained from the data subject) shall be provided:
     1. within a reasonable period after obtaining the personal data - up to 30 days, or
     2. at the latest at the time of the first communication to that data subject, or
     3. if a disclosure to another receiver is envisaged - at the latest when the personal data are first disclosed.
  6. Obligation to provide information shall be performed by:
     1. containing information clauses in all kinds of templates (applications, question form, contracts, etc.)
     2. placing information clauses in places publicly available, where stakeholders are given assistance,
     3. putting information clauses on the company's website;
     4. sending information clauses in electronic or traditional form, following contact made by the data subject,
     5. providing relevant information during verbal communication, where possible, or fulfilling information duty via the aforementioned methods.

# Data redundancy and data anonymization

* 1. To meet the purpose of the data processing, maximum scope of data body has been determined.
  2. Regardless of the legal basis for the discussed purposes, persons can submit to MDH documents containing data being redundant to these purposes.
  3. It is allowed to immediately anonymize or erase submitted documents from the MDH resources.
  4. To perform this, it is possible to:
     1. redact redundant data on the documents, which also contain data necessary to meet the given purpose, wherein such redaction must be permanent with no possibility to restore redundant data;
     2. erase data by destroying the document in a shredder or deleting files stored on the computer or in e-mails, including the "trash";
     3. return redundant data to its sender - if original document is available.
  5. If redundant data are being repeatedly submitted for a given purpose, BUM in cooperation with the DPS can:
     1. prepare forms, which limit possibility to provide redundant data;
     2. in a proper announcement inform about the principles of the decisions being taken in relation to a given purpose, so that it is clearly stated, that no extra data needs to be submitted;
     3. directly request the persons not to deliver redundant data.

# Exercising data subject's rights

* 1. Data subjects hold the rights specified in chapter III of the GDPR. They have right to request from MDH access to their personal data and relevant information on its processing, right to rectification, erasure and portability of data, right to restriction of processing, as well as right to object to processing of the personal data.
  2. Any request from the data subject, concerning the right he/she holds under GDPR, must be fulfilled according to the "Exercising data subject's rights procedure".
  3. If in doubt, in terms of the scope of information to be provided or request relevance, the request must be consulted with BUM or DPS.

# Principles of giving access to personal data

* 1. Access to the processed data are given by MDH only to the persons and entities authorised under applicable provisions of law.
  2. Unless otherwise specified by law, prior to accessing to the processed data one is obliged to submit written application with relevant justification.
  3. The application must contain information necessary to find personal data, determine the scope and purpose of personal data processing, as well as relevant legal basis.
  4. The application is examined by BUM, and in in doubt, by DPS.
  5. In matters in dispute, relevant decision is taken by the Management Board.
  6. The Board may refuse to give access to personal data, if this could result in infringement of personal interest of data subjects, other persons or if this is illegal.

# Principles of personal data entrusting

* 1. MDH can entrust personal data processing to other entity only under agreement concluded in writing or under applicable provisions of law, which govern such entrusting.
  2. Entrusting agreement is required whenever personal data is transferred or collected by the external entity.
  3. Should an employee of the external entity be granted access to the personal data, which is processed within the MDH premises, it is necessary to grant relevant authorisation.
  4. If entrusting agreement referring to GDPR procedures is concluded with the external entity, such entity becomes the Processor (P). Discussed agreement must specify:
     1. the purpose of processing, subject to the provision, that no other purpose is acceptable;
     2. the scope, categories and type of entrusted data;
     3. liability of the parties, including liability for fulfilling contractual obligations and satisfying applicable provisions of law - in particular in terms of suitable technical and organisational security measures to be implemented;
     4. obligation of the Processor to authorise other persons, who process data on his behalf, and to oblige them to keep all data confidential;
     5. ban to use other sub-contractors without the written consent or annex to the contracts;
     6. obligation of the Processor to fulfil MDH duties of the personal data controller, which cover exercising of the data subject's rights, providing information on the processing methods, as well as information necessary to perform risk and impact assessment;
     7. report all incidents or incident suspicions, providing all necessary information, which guarantee incident reporting compliant with the provisions of law;
     8. a method of confirming observance of the law and security principles, including monitoring and auditing competences granted to the Processor;
     9. obligation to erase or return entrusted personal data following expiration or termination of the agreement.
  5. Template of the Personal Data Entrusting Agreement is included in the Annex 4.
  6. Each Processor and possible sub-contractors are entered into the register of processors kept by the PDS, as specified in the Annex 3.

# Registering of the personal data processing

* 1. All persons responsible for personal data processing are obliged to inform the Management Board about:
     1. plans to develop new personal data processes or to resign from the old ones;
     2. introducing changes in the existing processes, e.g. changing the scope of the processes, as required by the applicable provisions of law;
     3. planned changes in the scope of data processing, such as developing new processes or resigning from the old ones.
  2. Using the aforementioned information, an employee assigned by the Management Board updates Register of Processing or assesses planned changes with regard to possible, additional security measures to be implemented.
  3. The said Register shall be kept in electronic form as specified in the template of Annex 6 to the Personal Data Security Policy.

# Security measures in the rooms

* 1. All rooms, where personal data are processed, are provided with locked doors and fire fighting measures.
  2. Access to the building is monitored using alarm system.
  3. All document containing personal data must be kept in cabinets and drawers provided with locks.
  4. Keys to the aforementioned locks are kept only by persons authorised to process personal data within the scope specified in the relevant authorisation.
  5. During off-hours the building is secured by the intervention group.
  6. Any third parties may enter the room, where personal data is stored, exclusively in the presence of authorised person. In particular, it is strictly forbidden to leave the third parties in these rooms without supervision.
  7. If an authorised person needs to leave the room, it is required to lock the room, so that no access of the third parties is possible.
  8. The last person leaving the rooms and the building must check, if the doors are locked.

# Print-out of the documents containing personal data

* 1. It is forbidden to leave the printers without supervision, if personal data from the IT system is being or is planned to be printed, unless the access to the rooms with printers is suitably restricted.
  2. If possible, print-outs from the IT system containing personal data should be stored in the cabinets with locks.
  3. It is absolutely obligatory to destroy any print-outs, notes, copies of documents, etc. which are useless and which contain personal data, in a manner which makes it impossible to restore their content.

# Sanctions

* 1. Failure to comply with the security principles described in the ISMS and in the relevant provisions of law specifying personal data protection, shall be interpreted as breach of professional duties and is likely to initiate disciplinary procedure or sanctions specified in the Law or GDPR.

**Łódź, 25th May 2018**  **the Management Board:**

Piotr Baczyński

Anetta Włodarczyk

Mariusz Gierałt