KPT, PO Box, CH-3001 Bern
kpt.ch

KPT Information System Processing Policy

(In accordance with Art. 21 OFADP and Art. 84b HIA)

Contents

1 Background 2

2 Contents 2

3 System documentation 2

3.1 Affected organisational units 2
3.2 Interface description 2
3.3 Data source 3
3.4 Data recipient 3
3.5 Data disclosure purposes 3
3.6 Scope of data transmission 4

4 Organisational chart of the system operator 4

5 Responsibilities 4

6 Documentation of the planning, implementation and operation of the data file 4

7 Registration of the data file with the FDPIC (Art. 16 OFADP) 4

8 KPT information system process documentation 5

9 Control procedures as well as technical and organisational measures in accordance with Art. 20 OFADP 5

9.1 Physical access control 5
9.2 System access control 5
9.3 Control of data recording (logging) 5
9.4 Data media control/storage control 5
9.5 Data transfer control 6
9.6 Disclosure control 6
9.7 User control 6

10 Description of the data fields and the organisational units that have access to them (Art. 21 (2)(e) OFADP) 6

11 Nature and extent of access by users of the data file (Art. 21 (2)(f) OFADP) 6

12 Training of data file users 6

13 The data processing procedures, in particular the procedure for the rectification, blocking, anonymisation (pseudonymisation), storing, safeguarding, archiving or destruction of data (Art. 21 (2)(g) OFADP) 7

14 Configuration of the information technology used (Art. 21 (2)(h) OFADP) 7

15 Procedure for exercising the right of access (Art. 21 (2)(i) OFADP) 7

16 Publication 7

1 Background

KPT Krankenkasse AG is the controller of the **KPT information system**, an automated data file that must be registered with the Federal Data Protection and Information Commissioner (FDPIC) and contains sensitive data and personality profiles. The purpose of the data file is the management and processing of health and accident insurance in connection with compulsory and supplementary health insurance under the IPA.

Based on Articles 11 and 21 of the Ordinance on the Federal Act on Data Protection (OFADP), a Processing Policy must be drawn up for the data file. In accordance with Art. 84b of the Health Insurance Act (HIA), the regulations must be submitted to the FDPIC for evaluation and be publicly accessible.

2 Contents

This Processing Policy describes the data processing and control procedures and operation of the KPT information system. It also contains the information required for the reporting obligations (Art. 15 OFADP) as well as information about the body responsible for the protection and security of the data (the controller), the source of the data, the purposes for which the data is regularly disclosed, the control procedures and in particular the technical and organisational measures in terms of Art. 20 OFADP, the description of the data fields and organisational units that have access to them, the access by users of the data file as well as the nature and extent of such access, the data processing procedures, in particular the procedure for the rectification, blocking, anonymisation, storing, safeguarding, archiving or destruction of the data, configuration of the information technology used as well as the procedure for exercising the right of access.

This Processing Policy also applies to the independent data reception service, as defined in Art. 59a HIO, which is operated internally at KPT.

3 System documentation

3.1 Affected organisational units

KPT Krankenkasse AG is the system operator and, as the controller of the automated data file KPT information system, the body responsible.

3.2 Interface description

KPT has outsourced some services, which can include the processing of personal data, to the outsourcing partners for IT operations, as well as the partners for document processing and postal solutions, based on Art. 84 HIA. Data protection-compliant processing as well as data security are regulated in the respective contracts and SLAs. Some of the IT partners are also certified to various ISO standards (in particular ISO 9001: Quality Management System and ISO/IEC 27001: Information Security Management System).

As the controller of the data file, KPT remains responsible for compliance with data protection for any data processed by third parties (Art. 22 OFADP).

KPT maintains interfaces to the data recipients and data suppliers described below for the management and processing of health and accident insurance in connection with compulsory health insurance under the HIA.

Recipient/supplier	Purpose	Sensitive personal data	Transmission
Banks/financial services providers	Payment transactions	No	Automatic/manual
Public authorities/courts	Art. 82 HIA Art. 84a HIA	Yes	Manual
Data hub	Benefit processing under HIA	Yes	Automatic
External printworks	Customer magazine	No	Automatic
Gemeinsame Einrichtung under HIIA	Exposure to risk	No	Manual
HMO partners	Gatekeeping, contractual compliance	Yes	Automatic
Cantons	Individual premium reduction	Yes	Manual
Provider	Art. 84a HIA	Yes	Automatic/manual
Telemedicine service provider	Health care	Yes	Automatic
Partner recourse	Recourse	Yes	Automatic
Santésuisse	Information, ZSR, data pool	No	Automatic
Social insurer	Art. 84a HIA	Yes	Manual
VEKA	Insurance card (HIA Art. 42a, ICO)	Yes	Automatic
Insured persons	Information	Yes	Automatic/manual
Central register of contracts (ZVR)	Information	No	Manual

3.3 Data source

Data can be transmitted by health service providers, insured persons, other social insurance providers, public authorities and financial service providers.

3.4 Data recipient

The recipient of the data is KPT Krankenkasse AG. Personally addressed documents (especially management and medical examiner documents) are sent directly to the intended recipients at KPT. Other documents (letters, forms and bills) are digitised, structured and transcoded by the document processing partner (outsourcing partner) and transmitted to the KPT information system or workflow.

When billing DRG-based inpatient care services, the provider systematically submits the data records containing the administrative and medical data in accordance with Article 59 (1) HIO together with the bill to the independent data reception service of KPT in accordance with Article 59a HIO.

Individual data processing procedures are documented in internal process documents.

3.5 Data disclosure purposes

Activities relating to compulsory health insurance in accordance with the Health Insurance Act (HIA) are the primary purpose for the transmission of data. For details, see the interface description (3.2).

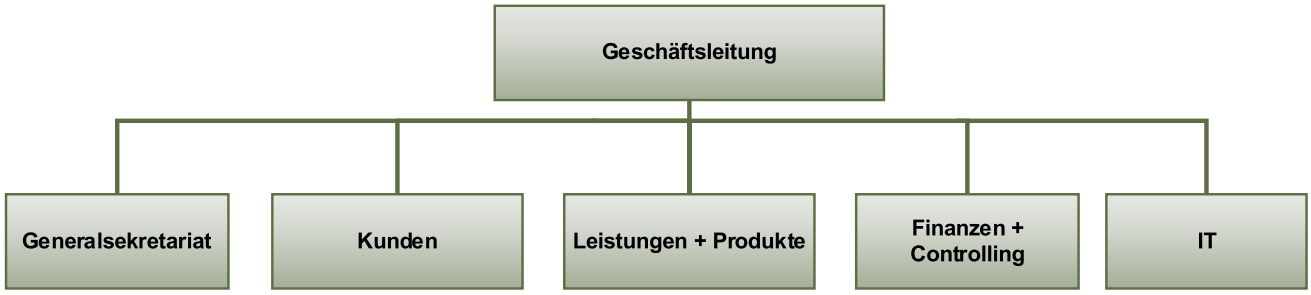
3.6 Scope of data transmission

The interface description (3.2) details which data is passed on to which recipients. The data is used exclusively for the following purposes:

- Special administrative assistance pursuant to Art. 32 (2) GSSLA and Art. 82 HIA
- Information and advice in accordance with Art. 27 GSSLA
- Inspection of files in accordance with Art. 47 GSSLA
- Data disclosure within the meaning of Art. 84a HIA.

Further information will only be disclosed in individual cases with the consent of the insured person. Moreover, data is transmitted only in compliance with the principles set out in Art. 4 et seq. of the Federal Act on Data Protection (FADP) and where appropriate and proportional to do so.

4 Organisational chart of the system operator



5 Responsibilities

As the controller of the data file, the Management Board of KPT Krankenkasse AG is responsible for data protection and data security. Data protection and data security activities are the responsibility of the governance functions (Data Protection, Corporate Security, Compliance, and Integrated Risk and Control Management). The persons holding these governance functions are integrated into control processes and are responsible for advising the Management Board and issuing relevant guidelines.

6 Documentation of the planning, implementation and operation of the data file

Operation of the data file is documented in an appropriate form.

The technical system components are documented in operating manuals.

The HERMES project management method is used for managing and documenting the planning and implementation of (life cycle) updates and further development.

7 Registration of the data file with the FDPIC (Art. 16 OFADP)

In accordance with Art. 11a (5)(e) FADP, KPT Krankenkasse AG has designated a data protection officer to independently monitor the company's compliance with data protection rules and keep a directory of the data files. KPT is thus exempted from the obligation to register the data file with the FDPIC.

8 KPT information system process documentation

The data processing procedures of the KPT information system are documented in the central process management tool and accessible to all KPT employees.

9 Control procedures as well as technical and organisational measures in accordance with Art. 20 OFADP

9.1 Physical access control

To prevent unauthorised access onto KPT premises, the buildings can only be accessed by KPT employees in possession of a badge or key.

The office premises may only be accessed for work purposes. Unknown persons will not be granted access to the building. In case of doubt, persons will be required to provide proof of their identity.

Visitors are required to register with reception and provide proof of their identity. They will be collected from reception by a KPT contact person and accompanied for the duration their visit. Building access is regulated in internal instructions.

9.2 System access control

KPT employs a multi-level security infrastructure for access to the KPT information system. All employees have a system login.

Access to the system is controlled by role-based authorisation and documented in authorisation concepts and an access matrix (Art. 21 (2)(e) OFADP).

The definition and implementation of authorisation concepts restricts access to data files on a need-to-know basis (for the performance of duties in accordance with Art. 84 HIA), preventing unauthorised access, modification and deletion.

Employees who have access rights for the performance of their duties are issued with specific guidelines to ensure the correct processing of data.

9.3 Control of data recording (logging)

All physical and system access is logged to ensure traceability.

KPT maintains a log of the most important activities performed. These logs are analysed anonymously by KPT to monitor compliance with the usage rules.

If abuse is detected or suspected, the log reports are analysed in detail. If evidence of abuse is found, appropriate sanctions will be taken. KPT employees are informed of this procedure.

9.4 Data media control/storage control

KPT also takes appropriate measures to prevent unauthorised persons from reading, copying, modifying or removing data from the KPT information system as well as unauthorised memory entries and the unauthorised access, modification or deletion of stored personal data.

As indicated above, physical access control prevents unauthorised external persons from entering KPT buildings, which in turn prevents any data processing by unauthorised external persons. To prevent unauthorised data processing by KPT employees, KPT uses technical measures to restrict or prevent access to data that is not required by employees for the performance of their duties under the HIA (Art. 84 HIA). More information on data access restrictions is provided in section 11 of this policy.

Employees must also comply with various policies and instructions on correct data processing. These include the data protection policies, which educate the employees on how to process data correctly.

Some system changes made by employees are traceable (see 9.3).

9.5 Data transfer control

KPT implements technical and organisational measures (such as encryption, HIN Mail or e-mail handling instructions) to prevent unauthorised data access or tampering during the transfer of personal data (by e-mail, for example) or the transportation of data media.

9.6 Disclosure control

The recipient of personal data is verified using manual or technical means.

9.7 User control

See 9.2

10 Description of the data fields and the organisational units that have access to them (Art. 21 (2)(e) OFADP)

Role-based access authorisation is used to control access to the KPT information system. An access matrix specifies the nature of access to the KPT information system for the specific roles.

11 Nature and extent of access by users of the data file (Art. 21 (2)(f) OFADP)

Only those employees who actually need access to the KPT information system will be granted this access. After being assigned a user profile (see 9.2 above), employees are given their personal access credentials, which must not be disclosed to third parties. Employees will be given either read or write access, as appropriate for their respective role.

MCD data that is received and processed automatically by KPT's independent data reception service is not accessible to KPT employees. If bills are diverted by the data reception service for review, the employees assigned to review the case will have access to the bills and associated MCD until the case is closed. Access to the MCD will be revoked once the case is closed.

Requests for authorisation must be approved by the employee's manager and the authorisation owner. Authorisations must be removed from employees if no longer required for the employee's assigned duties.

12 Training of data file users

All users of the KPT information system are given relevant data protection and application-related training. This means that all new KPT employees have to complete training both in data protection and on the KPT information system applications. KPT also requires employees to complete an e-learning module on data protection.

Users of the KPT information system are guided by various role-based application manuals for the system, as well as data protection policies.

13 The data processing procedures, in particular the procedure for the rectification, blocking, anonymisation (pseudonymisation), storing, safeguarding, archiving or destruction of data (Art. 21 (2)(g) OFADP)

Any data that has been modified by a KPT employee is documented in the system (see 9.3 above). To ensure the traceability of the data processing, the old and the new status after the modification are always visible.

The data processing procedures are documented in specific instructions, policies and manuals.

14 Configuration of the information technology used (Art. 21 (2)(h) OFADP)

The hardware and software used by KPT, in agreement with outsourcing partners, complies with international standards and is inspected periodically by independent auditors (ISAE 3402; ISO 27001).

Documentation on the configuration of the information technology used for the KPT information system is held at the IT department and the outsourcing partners of KPT and is updated as and when necessary.

15 Procedure for exercising the right of access (Art. 21 (2)(i) OFADP)

Requests for information pursuant to Art. 8 FADP must be submitted to the data protection officer:

KPT
Datenschutz
Wankdorfallee 3
3014 Bern

datenschutz@kpt.ch

16 Publication

In accordance with Art. 84b HIA, this policy is published online at kpt.ch.