ipro plan®
Planungsgesellschaft mbH
Beratende Ingenieure und Architekten

iproplan®

Privacy guidelines

Date: 01.06.2018

Table of Content

1. Fundamentals and target

The protection of private data is of major importance to iproplan®. The collection, use and processing of data related to employees, applicants, clients and other business partners is hence implemented in accordance with the valid legal provisions of the General Data Protection Regulation (GDPR) of the European Union (EU). The target is to ensure a responsible data security during all business operations.

2. Principles relevant to private data processing

According to the guideline, private data concerns every information that refers to a natural person (identified or identifiable). This can be name, address, date of birth, mail addresses, telephone numbers, but also identification numbers of every type (health insurance, social insurance, ID card, enrolment ID, …), bank data, information about personal characteristics or backgrounds and many more.
Personal data are only allowed to be processed if a legal regulation allows the processing, if the processing is prescribed by law, or if the person concerned gave an explicit authorisation.

The following basic principles are to be considered for the handling of these data:

a) **Fairness and legitimacy**
   The personal rights of the affected person have to be protected when processing private data. The data have to be collected and processed in a fair and legal manner.

b) **Proper purpose**
   Personal data processing is only allowed for such purposes that were specified prior to the data collection. Subsequent changes of the purposes have to be justified.

c) **Transparency**
   The affected person has to be informed about the handling of his / her data. Nature, purpose, extent and duration of the data use shall be clearly identifiable.

d) **Deletion**
   If there is no legal framework that justifies the storage and processing of personal data and / or if the affected person did not give explicit authorisation to do so, the personal data have to be deleted.

e) **Factual correctness and topicality**
   Personal data have to be stored correctly, completely and up to date if required and this guaranteed by adequate measures to be put in place.

f) Confidentiality and data security

Private data have to be handled confidentially. They have to be protected against unauthorized access, illegal processing and transmission as well as against their change or destruction via appropriate organizational and technical measures.

g) Right to information and revocation

Information about the collection, processing or use of private data at iproplan® can be obtained by the responsible privacy officer. Given approvals can be revoked at any time. Persons concerned may require their data's deletion.

3. Legitimacy of data processing

The collection, use and processing of private data is allowed if one of the following general permissions is available. This will also be valid if the reason for the data's collection, use and processing changes.

4. Data handling from clients, interested parties and partners

Private data coming from clients, interested parties and partners will be processed at iproplan® as follows:

- **Data processing in order to fulfil a contract**
  Private data from clients, interested parties or partners may be collected and processed in order to justify, implement or terminate a contract until the finished order processing. This also includes the contract partner's support if this is in connection with the contract's purpose. A respective written privacy note will be added to the contracts.
- **Data processing relevant to pre-contract measures**
  Prior to a contract signature (Initiation phase) private data processing is allowed in order to prepare offers as well as for the preparation of a contract signature and for the fulfillment of other wishes aiming at the contract signature and that were expressed by interested parties / clients. Interested parties / clients can be contacted during the initiation phase by using their data they had formerly provided to the company. Restrictions have to be taken care of if requested. A transmission of data belonging to clients, interested parties and partners to third parties not being involved will not occur.
- **Data processing for promotional purposes**
  Processing of data belonging to clients, interested parties and partners for promotional purposes is permissible if an interested party contacts iproplan® with a request for information.
- **Data processing based on the consent of the concerned party**
  Essentially, data processing based on the consent of the concerned party can be conducted. The declaration of consent has to made available in written or electronic form.
- **Data processing relevant to the fulfillment of legal requirements**
  Private data processing belonging to clients is permissible if legal requirements make this step necessary. The processing's nature and extent derive from the respective legal regulation.
- **Data processing based on justified interest**
  Private data may also be processed in order to achieve justified legal or economic interests of the company (e.g. enforcement of outstanding claims or prevention of contract breaches). Where appropriate it has to be verified whether one is dealing with interests of the concerned parties that have to be protected.

Additionally, the following provisions apply:

- **Processing of especially sensitive data**
  The processing of private data belonging to special categories according to article 9 GDPR will only apply after explicit written or electronic consent or based on legal regulations.
- **Automated individual decisions**
  iproplan® does not apply any procedure related to automated individual decisions according to article 22 GDPR.

- **User data and internet**

  A separate privacy statement on the iproplan® website informs about the collection, use and processing of private data. http://www.iproplan.de/datenschutz/en.

5. Handling of data belonging to employees

The handling of data belonging to employees is explained in detail in **Appendix 4 of iproplan®'s company agreement**. This privacy statement for employees informs comprehensively about the following points:

- the person responsible for data processing within the company (privacy officer)
- the legal foundation on which private data will be processed
- the purposes of private data processing within the company – in detail:
  -in order to fulfil a contract or pre-contract measures
  -in the framework of a justified interest of the company or third parties
  -in the framework of the employee's personal consent
  -in order to fulfil legal requirements or in public interest
- the processed data categories and their origin (if not received directly from the employee)
- the recipients and recipient categories of private data belonging to employees
- the duration of the data storage
- the processing of private data belonging to employees in a third country or by an international organisation
- the employee's privacy rights
- the data extent that the employee is bound to provide
- the implementation of purely automated decision makings (accord. to art. GDPR)
- the employee's right to objection (accord. to art. 21 GDPR)

The company makes sure that all employees receive this information.

6. Handling of data belonging to applicants

In order to initiate working relationships private data belonging to applicants may be collected and processed.
Each applicant will be informed (in written or electronic form) about the collection, use and processing of his / her data in the framework of the application process. The following principles apply in detail:

- **Data collection**

The data enumerated below will be collected, processed and stored in our internal applicant management system in the framework of the application:
Surname, first name; address; telephone number; e-mail address; submitted application documents (cover letter, CV, diplomas, certificates etc.)

- **Purpose of the data collection, use of applicant data**

The collection and processing of private applicant data will exclusively be conducted for the recruitment purposes within our company. The data will generally be transferred only to the responsible persons and departments being in charge of the concrete recruitment procedure within the company. Any use beyond this or data transmission to third parties will not occur.

- **Duration of private data storage belonging to applicants**

Data belonging to applicants will generally be deleted three months after the finalisation of the recruitment process at latest. This is not the case if legal requirements oppose the deletion, if further storage serves legal evidence or if the applicant gave his / her explicit consent in written or electronic form.

- **Data storage for future job advertisements**

If the company cannot offer a vacant position to the applicant, yet the applicant's profile might be of interest for future vacant positions, the applicant's private data may be stored in our internal applicant's management system if the applicant gave his / her explicit consent to such a storage and use in written or electronic form.

- **Right to information and revocation**

For questions related to the collection, processing or use of private data or for information, corrections or deletion of data, as well as for the revocation of given permissions, applicants may refer to the privacy officer in charge (for contact details, please refer to section 7).

7. The privacy officer

The company appoints a corporate privacy officer (PO) pursuant to the GDPR.

The main focus will be the compliance with the legal requirements related to data security as well as the handling of private data within the company in compliance with data security. In this framework, the following tasks have to be fulfilled according to art. 39 GDPR:

a) Information about the current duties relevant to data security and giving advice to resolve data privacy issues;
b) Monitoring and compliance with legal requirements relevant to data security (GDPR, Federal Data Protection Act, as well as other legal requirements) as well as with the privacy regulations within the company incl. allocation of responsibilities, sensitisation and training of employees;
c) Advising with privacy impact assessment if required (art. 35 GDPR) and monitoring of its implementation;
d) Cooperation with the regulatory authorities and responsibility to consult the authorities for questions related to data security;
e) Contact person for affected persons and employees for all aspects in relation to the processing of their data as well as for the protection of their rights.

In addition to these tasks, the PO has an advising and supporting function. Especially to be mentioned: supporting the responsible persons when establishing processes or documentation in order to fulfil comprehensive duties related to accountability, supporting reporting obligations in case of data breaches as well as the fulfillment of the rights of affected persons (right to information, correction, limitation or deletions of data).

The PO leads an inventory about the data processing procedures and proves the handling of this inventory on a regular basis. The fulfillment of the tasks as corporate privacy officer will be conducted independently. The PO will report to the responsible management board (regularly, one time per year minimum).

Contact information PO:

iproplan® Planungsgesellschaft mbH
betriebliche Datenschutzbeauftragte
Andrea Schilling
Bernhardstr. 68
09126 Chemnitz
E-Mail: dsb@iproplan.de

8. Privacy monitoring and responsibilities

The company provides the organisational, technical and the personnel-related framework in order to ensure the appropriate data processing by taking into consideration the data security accord. to GDPR.
The heads of department a required to ensure the appropriate processing of private data in their respective area of responsibility. The management board will be responsible for the data processing in the administration department (“Zentrale Aufgaben).

Employees that have to be very sensitive regarding the handling of private data due to their profession (IT administration, human resources, heads of department, management) are especially required to handle private data confidentially and to comply with privacy guidelines. This obligation has to be recorded.

Trainings for the correct handling of private data by complying with the legal requirements according to GDPR will be held for the employees with the participation of the PO and the respective responsible persons. All trainings and obligations will be recorded and will be part of internal and external audits in the framework of iproplan®’s quality management system.

All work processes and operations within the company are defined in the quality management manual. An inventory about the processing procedures within the company regarding the protection of private data will be added to these work processes. The handling of private data in the framework of all operational processes is generally subject to the requirements of the GDPR.