

**iproplan**<sup>®</sup>  
**Privacy guidelines and**  
**Information for affected parties according to art. 13 and 14 GDPR (DSGVO)**

**Status: 01.07.2020**

## Table of Content

1. Fundamentals, target, responsibility .....	3
2. Principles relevant to processing of private data.....	3
3. Data handling from project partners, clients, interested parties and partners .....	4
4. Data handling from applicants.....	6
5. Handling of data belonging to employees.....	7
6. Rights of affected people .....	7
7. The privacy officer .....	7
8. Implementation of the GDPR within the company.....	8

# 1. Fundamentals, target, responsibility

The protection of private data is of major importance to iproplan<sup>®</sup>. The processing of data related to employees, applicants, and project 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.

## Responsible for data protection:

**iproplan**<sup>®</sup> Planungsgesellschaft mbH

represented by Managing Director Dipl.-Ing. Jörg Thiele

Bernhardstr. 68, 09126 Chemnitz

[info@iproplan.de](mailto:info@iproplan.de), Tel. 0371/5265-0

# 2. Principles relevant to processing of private data

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.

The following principles apply to the handling of these data according to GDPR (ref. esp. art. 5 paragraph 1 and art. 9):

- Fairness and transparency
- Proper purpose
- Data minimisation
- Correctness
- Limitation of data saving
- Integrity and confidentiality

All data processing actions within the company are being recorded (register on processing activities, ref. art. 30 GDPR); new processes will undergo a risk analysis (impact assessment on privacy accord. to art. 35 GDPR if applicable). For processing activities on behalf of **iproplan**<sup>®</sup>, data processing contracts are being signed handling the contract-relevant data; all suppliers will be checked regarding their compliance with data security requirements (ref. art. 29 GDPR).

### 3. Data handling from project partners, clients, interested parties and partners

iproplan<sup>®</sup> processes private data from project partners, clients, interested parties and partners as follows:

#### **Purposes and legal basis:**

The data processing within project contexts as well as from clients, interested parties and parties usually applies

- in order to fulfil and execute contractual requirements as well as pre-contract measures,
- in order to fulfil legal requirements for **iproplan**<sup>®</sup> or
- in order to preserve legitimate interests for **iproplan**<sup>®</sup>, e.g. for new project applications with contract partners or third parties (references) (ref. art. 6 paragraph 1 esp. b, c, f GDPR).

A deviating legal basis only applies in accordance with GDPR.

#### **Categories of personal data that are being processed:**

Data are being processed from employees of respective contractual and/or project partners that the relevant partner appoints for contract execution purposes, mainly: surname, first name, academic title if applicable, professional designation, position within the company, power of representation, business address, business telephone number, business mobile number, business e-mail address.

#### **Categories of recipients of personal data:**

- iproplan<sup>®</sup> employees being appointed for the execution of contracts/projects
- if applicable employees from sub-consultants or other project partners with whom iproplan<sup>®</sup> is in contact for the execution of contracts/projects
- if applicable employees from potential clients upon whom iproplan<sup>®</sup> applies for new projects
- if applicable employees from regulatory authorities and auditors with whom iproplan<sup>®</sup> is in contact in order to fulfil its legal duties
- if applicable employees from professional liability insurance companies, law firms, and courts with whom iproplan<sup>®</sup> is in contact in order to enforce its interests

#### **Source of personal data:**

The data normally originates from the communication with the contractual partner, i.e. the data has been provided by the contractual partner him/herself. Additionally, publicly accessible data from the respective partner's online presence are being used if applicable.

#### **Automated decision making / Profiling:**

not applicable

**Data transfer into third countries:**

Usually not applicable; if necessary for project execution, the parties concerned are being informed.

**Duration of data storage:**

Personal data in relation to contracts will be saved until the end of the defects' liability period against **iproplan**<sup>®</sup>, but at least 10 years by the end of the year in which **iproplan**<sup>®</sup> submitted the final bill to the Client.

Data storage or handling from project partners, clients, interested parties and partners which is necessary for the enforcement, assertion, performance or defense of legal claims, shall remain unaffected.

## 4. Data handling from applicants

iproplan<sup>®</sup> processes private data from applicants as follows:

### **Purposes and legal basis:**

The collection and processing of private data from applicants is exclusively conducted for recruitment purposes within the company, i.e. in order to initiate employments (usually art. 6 paragraph 1 b).

A deviating legal basis only applies in accordance with GDPR.

### **Categories of personal data that are being processed:**

The data enumerated below will be 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.).

### **Categories of recipients of personal data:**

The data will generally be transferred only to the responsible persons and departments being in charge of the concrete recruitment procedure within the company.

### **Source of personal data:**

The applicant him/herself provides his/her personal data.

### **Automated decision making / Profiling:**

Not applicable.

### **Data transfer into third countries:**

Not applicable.

### **Duration of data storage:**

Data belonging to applicants will generally be deleted 6 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.

## 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**. The company makes sure that all employees receive this information.

## 6. Rights of affected people

People affected from data storage have the right to get informed about their personal data being processed, as well as the right of correction, deletion or limitation of the processing of their data (ref. to art. 15, 16, 17, 18, 20 GDPR).

Further, affected people have the right to appeal upon the regulatory authority (Sächsischer Datenschutzbeauftragter (Privacy Officer of Saxony), Devientstr. 1, 01067 Dresden, [saechsdsb@slt.sachsen.de](mailto:saechsdsb@slt.sachsen.de), Tel. +49(351)4935401).

We recommend to always direct demands and complaints to our corporate privacy officer first (contact data in section 7).

## 7. The privacy officer

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

The PO will mainly supervise the compliance with the legal requirements related to data security as well as the handling of private data within the company according to art. 39 GDPR.

Additionally, the corporate privacy officer will function as contact person for affected people and employees in relation to all processes pertaining to data processing and exercising their rights.

### Contact details PO:

iproplan® Planungsgesellschaft mbH  
Betrieblicher Datenschutzbeauftragter  
Bernhardstr. 68  
09126 Chemnitz  
Tel.: 0371/5265-0; E-Mail: [dsb@iproplan.de](mailto:dsb@iproplan.de)

## 8. Implementation of the GDPR within the company

The company provides the necessary 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.

All employees – accord. to work task and data categories to be processed - will be trained on a regular basis for the proper handling of personal data and for compliance with the legal requirements related to data protection.

The company's management board, the area managers as well as the heads of department are additionally required to ensure the appropriate processing of private data in their respective area of responsibility.

Potential violations of the data protection requirements (data privacy incidents, misplacements) will undergo a comprehensive risk analysis. The affected person will be informed accordingly, and the incident reported to the responsible regulatory authority within 72 hours if applicable.

All processes related to data protection as well as technical-organisational measures for the compliance with the requirements pertaining to data protection in all areas of the company are part of internal and external auditing in the framework of **iproplan**<sup>®</sup> quality management and are continuously being documented, reviewed and adapted.