Data Protection Policy

All3DP GmbH

Ridlerstr. 31A
D - 80339 München

November 2020

Data Protection Policy All3DP GmbH

Contents

Data Protection Policy All3DP GmbH

Foreword from Management

As a globally operating company, All3DP GmbH is obligated to comply with the data protection laws of the Federal Republic of Germany, the European Union and worldwide.

The company offers editorial content and purchase recommendations on everything to do with the 3D printing market via its website and provides visitors with a platform that facilitates the placement of 3D printing orders.

All3DP processes the data of the website visitors and platform users that could also reveal their online patterns and living situation.

Since May 2018, the European Union's General Data Protection Regulation (EU GDPR) has been in full force and, along with a few national regulations, forms the basis for the processing of personal data for all residents of the European Union and across national borders outside the EU.

For this reason, All3DP has prepared a Data Protection Policy that is designed to help its employees and partners to carefully and safely navigate the processing of the masses of personal data and to accurately assess any possible risks for the data subjects.

All3DP's Management stands behind this policy.

All staff members and partners are therefore required to internalize the provisions of this policy and heedfully apply them in their daily work.

On behalf of the Management team

Matthias Plica / CEO

Data Protection Policy All3DP GmbH

Scope and Objectives

All3DP GmbH undertakes to comply with data protection regulations in the Federal Republic of Germany, the European Union and worldwide as part of its corporate responsibilities.

This Data Protection Policy applies primarily to all of the company's employees and partners.

The policy is based on the European data protection principles and extends across all personal data processing. In countries where the data of legal persons is protected in the same way as is personal data, this Data Protection Policy equally applies to data of legal persons. Anonymized data, such as for statistical analyses or surveys, are not subject to the Data Protection Policy.

Compliance with data protection regulations is the basis for trusting business relationships and the All3DP's reputation as an attractive employer.

This policy ensures that the level of data protection (new Federal Data Protection Act in Germany (*BDSG-neu*) required by the European Union's General Data Protection Regulation (GDPR) and national laws is met, even for cross-border traffic to countries in which there exists no legally adequate level of data protection.

Changes to this Data Protection Policy is made in coordination with the Data Protection Officer.

The most current version of the Data Protection Policy can be accessed under "Data Protection" on All3DP's website.

The Data Protection Policy regulates the general handling of personal data in the company and is supplemented with specific rules for adhering to data protection in special situations.

Data Protection Policy All3DP GmbH

Terms und Abbreviations/Acronyms

The terms are defined in accordance with the term definitions given in individual, applicable laws, in particular those in Art. 4 of the GDPR. The most important terms are listed below:

Terms	Explanations
Personal data	Any information relating to an identified or identifiable natural person (hereinafter referred to as “data subject”). An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person.
Processing	Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, querying, use, disclosure through transmission, dissemination or making available otherwise, comparison/alignment or combination, restriction, erasure/deletion or destruction. Der term “processing” is brought into line with the terms process and procedure.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, patterns/behavior, location or movements.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided this additional information is kept separately and is subject to technical and organizational measures that ensure the personal data is not an identified or identifiable natural person.
Controller	A natural or legal person, government authority, institution or other body who/that, alone or jointly with others, determines the purposes and means of processing personal data. Where the purposes and means of such processing are determined by Union or EU Member State law, the data controller or the specific criteria for its appointment can be provided for by Union or Member State law.
Processor	A natural or legal person, government authority, institution or other body who/that processes personal data on behalf of the controller.
Recipient of data	A natural or legal person, government authority, institution or another body to whom the personal data is disclosed, regardless of whether it is a third party or not. Government authorities that may receive personal data as

	part of a specific investigation under Union law or the law of EU Member States are not considered recipients. The processing of the data by these particular authorities takes place in line with data protection regulations according to the specific processing purpose.
Third party	A natural or legal person, government authority, institution or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

The main abbreviations used in this policy are defined as follows:

Abbreviation	Explanation
Federal Data Protection Act / FDPA (*BDSG-neu*)	Act to adapt and implement data protection law to EU regulations and directives (*DSAnpUG-EU*). The national data protection laws for the implementation of the opening clauses from the General Data Protection Regulation / GDPR (*BDSG*).
DPO	Data Protection Officer
DPCo	Data Protection Coordinator
DPIA	Data Protection Impact Assessment (according to Art. 35 of the EU GDPR)
DPMS	Data Protection Management System
EU's General Data Protection Regulation (EU GDPR or GDPR)	Regulation (EU) 2016/679 (General Data Protection Regulations)
EU Privacy Regulation or ePR	The ePrivacy Regulation (currently still in draft)
ISMS	Information Security Management Systems (in accordance with ISO/IEC 27001)

Data Protection Policy All3DP GmbH

Organizational structure with regard to data protection within All3DP

The Data Protection Officer (DPO) at All3DP represents a professional body of the company is independent of instructions and works towards compliance with national and international data protection regulations. He or she is responsible for the data protection policy and monitors the company's compliance. A more detailed description of the DPO's responsibilities are defined in Art. 37 of the GDPR.

The Data Protection Officer is appointed by the Executive Managers of the company. From each of the departments "Editorial" and "Craftcloud" as well as "IT" and "Administration" a contact person (Data Protection Coordinator / DPCo) is assigned to the DPO to support him/her in data protection and data security activities.

The description of the duties of the Data Protection Coordinators are defined in more detail in the organizational structure overviews and include, at a minimum, the provision of timely information on data protection-related topics and risks concerning the respective departments as well as the participation in compliance to meet the required level of data protection in the company.

Every "data subject" may contact the Data Protection Officer or the Data Protection Coordinator with suggestions, inquiries, information requests or complaints regarding data protection or data security in processing personal data.

Inquiries and complaints are treated confidentially upon request and can be reported directly to the DPO.

Inquiries from supervisory authorities and data subjects must always be brought to the attention of the Data Protection Officer.

The Data Protection Officer can be reached at:

All3DP GmbH
c/o Data Protection Officer
Ridlerstr. 31A
D-80339 München

datenschutz@All3DP.de

Data Protection Policy All3DP GmbH

Principles of processing personal data

- **Lawfulness of processing, processing in good faith**

When processing personal data, the data subject's personality rights must be protected. Personal data may only be processed in a lawful manner and in good faith. The DPO checks for the legality of the processing of all personal data.

- **Transparency**

Personal data must be processed in a way that is transparent to data subjects. Data subjects must be informed about the type and effects of personal data processing in an appropriate, unambiguous and comprehensible way.

- **Purpose Limitation**

Personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Data minimization**

The processing of personal data must be relevant to the purpose and limited to what is necessary in relation to the purpose.

- **Accuracy**

The personal data must be factually correct and up to date. Appropriate measures must be taken to ensure that incorrect data can be deleted or corrected immediately.

- **Storage limitation**

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Therefore, retention or deletion periods must be defined and adhered to for all types of data processing.

- **Confidentiality and data security**

Personal data must be processed in a manner that ensures an appropriate level of security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, accidental destruction or accidental damage, using appropriate technical or organizational measures.

Data Protection Policy All3DP GmbH

Permissibility of personal data processing

All3DP website and craftcloud3d.com visitors

- **Data processing for performance of a contract**

Processing personal data on the website users, Craftcloud customers, partners and their staff or contact persons is justified when necessary for the performance of an existing or prospective contract. Potentially interested parties may be contacted for the purpose of initiating a contract using only the personal data provided by them.

If a data subject contacts the company to request information (e.g., a request to receive information material about a product or service), processing the personal data for the purpose of fulfilling his or her request is permitted.

- **Data processing for advertising purposes**

Customer loyalty or advertising measures are subject to additional legal requirements.

Processing personal data for the purpose of advertising or market and opinion research is permitted, provided that it is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected exclusively for advertising purposes, it is understood that the personal data is given voluntarily by the data subject. The data subject is to be informed about the voluntary nature of the provision of data for the express purpose of advertising. When communicating with the data subject, the data subject's consent to processing his or her data for advertising purposes must be obtained. As part of obtaining the data subject's consent, he or she should be given the option of choosing between available contact channels, such as postal mail, electronic mail and telephone.

If the data subject objects to the use of his/her data for advertising purposes, further use of that person's data for this purpose is not permitted, and the personal information must be blocked for any and all advertising purposes.

- **Consent to data processing**

Data processing is permissible if the data subject gives his or her consent. Before giving his or her consent, the data subject has to be sufficiently and verifiably informed.

For reasons of proof, the declaration of consent must always be obtained in writing or electronically. Under certain circumstances, such as when offering telephone support, consent can also be given verbally, which must be documented immediately.

If the data subject gives his/her consent in form of a written declaration that also relates to other issues, the consent request must be made available in a readily understandable and easily accessible form, clearly and plainly-worded, so that it can be easily distinguished from the other issues. The data subject must be informed of each new or additional type of processing or of each individual processing purpose and agree to each individually.

- **Data processing based on legal permission**

Processing personal data is also permitted if government regulations and laws requires, presupposes or permits data processing. The type and scope of data processing must be necessary for the data processing permitted by law and comply with these legal provisions.

- **Data processing based on legitimate interest**

Another lawful purpose for processing personal data occurs when processing is necessary for a legitimate interest pursued by All3DP or by a third party. Legitimate interests are usually of a legal (e.g., collecting outstanding receivables) or commercial nature (e.g., avoiding breaches of contract).

Personal data may not be processed on the basis of a legitimate interest if, in an individual case, there is any indication that the legitimate interest of the data subject outweighs the interest in the processing. Legitimate interest must be checked individually for each processing operation.

The reasons for the legitimate interests must be documented and indicated both in the processing summary and the respective data processing information documentation (data processing declaration on the internet or on forms).

- **Processing particularly sensitive data**

The processing of particularly sensitive personal data in accordance with Art. 9 of the GDPR is permissible only if required by law or if the data subject has given express prior consent. Processing this type of data is also justified if it becomes absolutely necessary in order to assert, exercise or defend legal claims against a data subject.

Considered particularly sensitive data is any information that in any way reveals a person's race, ethnic origin, political opinions, religious or ideological convictions or union membership as well as genetic data, biometric data for clear identification of a natural person, data related to health or to the sex life or sexual orientation of a natural person.

- **Automated individual decisions**

Automated processing of personal data, which is used to rate or measure a person's individual personality traits (e.g., creditworthiness), shall not be the sole basis for arriving at decisions with potentially negative legal consequences or significant impairments of any sort for the data subject. The data subject must be informed of the fact and the result of an automated individual decision and given the opportunity to respond.

- **User data and internet**

If personal data is collected, processed and used on websites or in apps, the data subject must be informed of this in data protection notices and, if applicable, cookie notices. The data protection notices and any cookie notices are to be integrated in such a way that they are easily recognizable, immediately accessible and permanently available to the data subjects.

If usage profiles are created (tracking) to evaluate website and apps usage patterns, data subjects must be informed of this in data protection and privacy notices. Personal data tracking is only allowed if national law permits this or if the data subject has consented. If tracking takes place under a pseudonym, the data subject should be given the option to opt out in the data protection notice.

If access to personal data is made possible on websites or apps in an area requiring registration, the identification and authentication of data subjects must be designed in such a way that appropriate protection is ensured for each access.

- **Data processing in the context of employment**

For employment purposes, personal data required for the conclusion, execution and termination of an employment contract may be processed.

When initiating an employment relationship, personal data of applicants may be processed. After rejection, the applicant's data must be deleted, taking into account time limits under the law of evidence, unless the applicant has consented to further storage for a later selection process. Consent is also required for the data to be used for further application procedures or before the application is passed on to other Group companies, subsidiaries or partners.

In the existing employment relationship, data processing must always be related to the purpose of the employment contract, unless one of the following conditions of permission for data processing applies.

If it is necessary to collect further information about the applicant from a third party during the initiation of the employment relationship or in the existing employment relationship, the respective national legal requirements must be taken into account. In case of doubt, the consent of the person concerned must be obtained.

For the processing of personal data in the context of the employment relationship, but which do not originally serve to fulfil the employment contract, a legal legitimation must exist in each case. These can be legal requirements, collective regulations with employee representation, employee consent or the legitimate interests of the company.

- **Data processing on the basis of legal permission**

The processing of personal employee data is also permitted if government legislation requires, presupposes or permits data processing. The type and scope of data processing must be necessary for the data processing permitted by law and comply with these legal provisions. If there is legal room for maneuver, the legitimate interests of the employee must be taken into account.

- **Collective regulations for data processing**

If processing goes beyond the purpose of contract execution, it is also legitimate if it is permitted by a collective regulation. Collective regulations are collective agreements or agreements between employers and employee representatives within the framework of the possibilities offered by the respective labor law. The regulations must extend to the concrete purpose of the desired processing operation and can be designed within the framework of the data protection law.

- **Consent to data processing**

Processing of employee data may take place on the basis of the data subject's consent. The declaration of consent is given voluntarily. Consent not given voluntarily is not legally effective. For reasons of proof, the declaration of consent must always be obtained in writing or electronically. In cases where this is not possible, consent can also be given verbally. One way or the other, consent issuance must be properly documented.

- **Processing based on legitimate interest**

The processing of personal employee data may also be carried out if this is necessary to realize a legitimate interest of the company. As a rule, legitimate interests are justified either legally (e.g., asserting, exercising or defending legal claims) or economically (e.g., valuing companies).

Personal data may not be processed on the basis of a legitimate interest if, in an individual case, there is any indication that the legitimate interests of the employee outweigh the interest in the processing. The existence of legitimate interests must be checked for each processing operation.

Control measures that require the processing of employee data may only be carried out if there is a legal obligation to do so or if there is a justified reason to do so. The proportionality of the control measure must also be examined if there is a justified reason for doing so. The legitimate interests of the company in the implementation of a control measure (e.g., compliance with legal provisions and in-house policies) must be weighed against any legitimate interests of the employee in the exclusion of the measure and may only be implemented if reasonable.

The legitimate interest of the company and the possible legitimate interests of the employees must be determined and documented before each measure is taken.

In addition, other requirements existing under government law (e.g., employee representation rights of co-determination and information rights of the persons concerned) may have to be taken into account.

- **Processing particularly sensitive data**

The processing of sensitive personal data, such as any information that in any way reveals a person's race, ethnic origin, political opinions, religious or ideological convictions or union membership as well as genetic data, biometric data for clear identification of a natural person, data related to health or to the sex life or sexual orientation of a natural person.

Due to federal law, additional data categories can be classified as particularly sensitive or the content of the data categories can be filled differently. Likewise, data relating to criminal offenses may often only be processed under special conditions stipulated by federal law. The processing must be expressly permitted or prescribed by federal law. In addition, processing may be permitted if it is necessary so that the responsible body can meet its rights and obligations in the area of labor law.

The employee can also voluntarily expressly consent to the processing.

- **Automated decisions**

Personal data automatically processed in employment situations to rate or measure a person's individual personality traits (e.g., as part of selection process or to evaluate skill profiles) shall not be the sole basis for arriving at decisions with potentially negative consequences or significant impairments of any sort for the employee concerned.

In order to avoid incorrect decisions, it must be ensured that a natural person check the facts in automated processes and that the results of this assessment serves as the basis for decision-making. The employee concerned is to be informed of the fact and the result of an automated individual decision and given the opportunity to respond.

- **Telecommunication und internet**

Telephone systems, e-mail addresses, internet as well as internal social networks are primarily provided by the company within the scope of the operational tasks. They are work equipment and a company resource. These resources may be used within the framework of the applicable legal regulations and the company's internal policies.

If use is permitted for private purposes, telecommunications privacy and the applicable national telecommunications law must be observed, insofar as they apply.

There is no general monitoring of telephone, e-mail or internet/intranet use. To prevent attacks against the IT infrastructure or individual users, protective measures can be implemented at the gateway into the All3DP's network that block technically harmful content or analyze the patterns of attacks. For security reasons, the use of telephone systems, e-mail addresses, the internet and intranet as well as the internal social networks can be logged into for a limited period of time.

Evaluations of personal data may only be carried out in the event of a concrete, justified suspicion of a violation of laws or the company's policies. These controls may be conducted only by investigating departments and in accordance with the principle of proportionality. The respective national laws are to be observed as well as the existing company regulations, such as the code of conduct.

Transmission of personal data

A transmission of personal data to recipients outside or within the company is subject to the permissibility requirements of processing personal data as defined under "All3DP website and craftcloud3d.com visitors" of this policy.

The recipient of the data must be obliged to use the data only for the specified purposes. In the case of data transfer to a recipient outside the company in a third country, the recipient must guarantee a data protection level equivalent to this Data Protection Policy.

This does not apply if the transmission is based on a legal obligation and is absolutely necessary for this.

If data is transmitted from a third parties to the company, it must be ensured that the data may be used for the intended purposes.

If personal data from an All3DP company located in the European Economic Area (EEA) is transferred to a company based outside the EEA (third country), the data-importing company is obliged to cooperate with the supervisory authority responsible for the data-exporting company with regard to all inquiries and to observe the findings of the supervisory authority in terms of the transferred data. The same applies to data transfers by All3DP companies from other countries.

Order processing and shared responsibility

Order processing exists when a contractor is commissioned with the processing of personal data without being assigned responsibility for the associated business process. Art. 28 of the GDPR applies here. In such cases, an agreement on order processing must be concluded with external contractors. All3DP retains full responsibility for the correct execution of data processing, its monitoring and protection of the rights of the data subject's rights.

If two or more responsible bodies jointly determine the means and purposes of the processing of personal data, then this falls under data processing according to Art. 26 of the GDPR, which requires a special contractual agreement.

- **Order processing in accordance with Art. 28 of the GDPR**

If orders are being processed according to Art. 28 of the GDPR, the contractor may only process personal data within the scope of the customer's instructions. When placing the order, the

following requirements must be observed; the commissioning department must ensure their implementation.

1. The contractor is to be selected according to his or her suitability to ensure the necessary technical and organizational protective measures.
2. The order must be placed in text form. The instructions for data processing and the responsibilities of the customer and the contractor must be documented.
3. The contractual standards provided by the DPO must be observed.
4. The customer must make sure that the contractor is in compliance with his or her obligations before commencing data processing. One of the best ways a contractor can prove compliance with the data security requirements is by submitting a valid certification. Depending on the risk of processing the data, control checks may have to be repeated regularly during the term of the contract.
5. In the case of cross-border order data processing, the respective national requirements for the transfer of personal data abroad must be fulfilled. In particular, the processing of personal data from the European Economic Area may take place in a third country only if the contractor can guarantee a data protection level equivalent to this Data Protection Policy. Suitable instruments can be:
    1. Agreement of the EU standard contractual clauses on contract data processing in third countries with the contractor and possible subcontractors.
    2. Participation of the contractor in a certification system recognized by the EU for the creation of an appropriate level of data protection (e.g., Privacy Shield procedure).
    3. Recognition by the responsible data protection supervisory authorities of the contractor's binding company rules to establish an appropriate level of data protection.

- **Processing according to Art. 26 of the GDPR (shared responsibility for processing)**

If the processing of the personal data is shared within the framework of Article 26 of the GDPR, the contracting parties determine, in the form of a transparent written agreement, who is responsible for meeting which obligations under the GDPR, in particular with regard to protecting the rights of the data subjects and who has which information obligations according to Art. 13 and 14 of the GDPR, if and to the extent that the respective tasks of the controller are not stipulated by legal regulations of the EU or the EU Member States to which the controllers are subject.

The agreement must include

1. The details of a contact point for the data subjects.

2. The respective actual functions and relationships of the jointly responsible controllers with respect to the data subjects.

Data protection through technical design and data protection-friendly default settings

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the varying probability of occurrence and severity of potential risks to the rights and freedom of natural persons associated with the processing of personal data, both at the time of determining the means to take appropriate technical and organizational measures for the processing as well as at the time of the actual processing, which are designed to effectively implement the data protection principles and to include the necessary guarantees in the processing in order to protect the rights of the data subjects and to meet the requirements of the GDPR.

All3DP implement appropriate technical and organizational measures to ensure that by default only the personal data, the processing of which is necessary for the respective specified processing purpose, is processed.

This obligation applies to the amount of personal data collected, the scope of processing this data, its storage period and accessibility. In particular, such measures include default settings to ensure that personal data is not made available to an infinite number of natural persons without intervention by the respective person.

These measures include, for example, the processing of pseudonymized data only, the use of special authentication measures (2-factor authentication), basic data protection-friendly default settings in checkboxes or the marking of information to be collected as voluntary.

Rights of the data subject

If a data subject exercises his or her right to access as defined in Art. 15 of the GDPR or his or her right to rectification or to object as stipulated in Art. 16 and 21 of the GDPR, the central processing is carried out by the Data Protection Coordinators and the Data Protection Officers. Access must be given within a period of 4 weeks.

The employees' right to access and to inspection is handled by the Human Resources departments.

It must be ensured that, upon request, the data subject's data is made available to him or her in a structured, commonly used and machine-readable format. The DPO and the IT department must agree in advance which standard meets the requirements and must be defined in a process description. Only that data has to be provided that was transmitted to All3DP by the data subject.

Information must generally be sent in writing to the address known to All3DP.

To safeguard the identity of the person requesting information, the ID check can be used if the address is unknown or there are legitimate doubts about the accuracy of the information.

Confidentiality of processing

Personal data is subject to data privacy regulation. The company's employees are prohibited from unauthorized collection, processing or use. Any processing undertaken by an employee without being entrusted with it in the course of the performance of his or her duties and without being authorized to do so is considered to be unauthorized. The need-to-know principle applies: Employees may only have access to personal data if and insofar as this is necessary for their respective tasks. This requires the careful division and definition of separate roles and

responsibilities as well as their implementation and maintenance within the framework of authorization concepts. This principle must be ensured by both your own IT department as well as in in order processing or software development processes.

Employees may not use personal data for their own private or commercial purposes, transmit the data to unauthorized persons or make the data accessible in any other way. Superiors must inform their employees of the obligation to maintain data secrecy at the beginning of the employment relationship. This obligation continues to exist even after the termination of the employment relationship.

Superiors must inform their employees of the obligation to comply with data privacy regulations at the beginning of the employment relationship. This obligation continues to exist even after the termination of the employment relationship.

All3DP provides special forms for this. Depending on the role in the company, every employee, but also external service providers, have to sign corresponding declarations of commitment, among others, to maintain absolute confidentiality when it comes to personal data (data privacy).

Security of processing

Personal data must be protected at all times against unauthorized access, unlawful processing or disclosure, and against loss, falsification or destruction. This applies regardless of whether the data processing is carried out electronically or in paper form.

Technical and organizational measures for the protection of personal data must be defined and implemented before new data processing procedures, in particular new IT systems, are introduced. These measures must be based on the state of the art, the risks posed by the processing and the need to protect the data.

The responsible division may, in particular, consult the Information Security Officer and the Data Protection Coordinator. The technical and organizational measures for protecting personal data are part of the company-wide information security management and must be continuously adapted to technical developments and organizational changes.

Data protection impact assessment (DPIA)

Where a type of processing personal data, in particular using new technologies and taking into account the nature, scope, circumstances and purpose of the processing, is likely to result in a high risk to the rights and freedom of natural persons, an assessment of the impact of the planned processing operations must first be carried out for the protection of personal data.

A single assessment may address a set of similar processing operations that present similar high risks.

The DPO, the departments responsible, their DPCos and IT are responsible for the implementation of the DPIA, which must be documented accordingly.

Data protection monitoring

Compliance with the Data Protection Policy and the applicable data protection laws is monitored regularly through data protection audits and other controls. The execution is the responsibility of the Data Protection Officer, the Data Protection Coordinators, divisions with audit rights or commissioned external auditors.

The results of the data protection checks must be communicated to the DPO. As part of the respective reporting obligations, Management is to be informed about the essential results. Upon request, the results of data protection checks have to be made available to the relevant data protection supervisory authority.

The data protection supervisory authority may also carry out its own checks on compliance with the provisions of this policy within the limits of its powers under national law.

All3DP's competent supervisory authority is currently:

Bayerisches Landesamt für Datenschutzaufsicht

Address: Promenade 18, 91522 Ansbach, Deutschland
P.O. Box: P.O. Box 1349, 91504 Ansbach, Deutschland
Telephone: +49 (0) 981 180093-0, Fax: +49 (0) 981 180093-800, Email: poststelle@lda.bayern.de

Data breach incidents

Every employee should immediately report any violations of this Data Protection Policy or other personal data protection regulations to his or her supervisor, the DPCo or the DPO.

The manager responsible for function or unit is required to inform the respective DPCo or DPO about data breach incidents.

Incidents to be reported (or that have become known):

a) unlawful transfer of personal data to third party
b) unlawful access to personal data by third parties or
c) personal data is lost

The company must be notified immediately so that data protection incident reporting obligations can be met according to national law.

Responsibilities and sanctions

Management is responsible for data processing in the company. It is thus obliged to ensure that the legal and data protection requirements contained in the Data Protection Policy are taken into account (e.g., national reporting obligations). It is Management's responsibility to ensure proper data processing that is in compliance with all data protection regulations by way of organizational, personnel and technical measures.

The implementation of these requirements is the responsibility of the responsible employees. In the event of data protection controls by public authorities, the DPO of the company must be informed immediately.

Those responsible for business processes and projects must inform the DPCos and/or the DPO in a timely manner about new processing of personal data. In cases where data processing projects may entail particular risks for the personal rights of the data subjects, the DPO of the company must be involved before the processing begins. This applies in particular to particularly sensitive personal data. Managers must ensure that their staff is receives data protection training to the extent necessary. Abuse of personal data processing or other violations of data protection laws are also prosecuted in many other countries and can result in claims for damages.

Violations for which individual employees are responsible can lead to labor law sanctions/penalties.