Commitment to Confidentiality according to the GDPR

For your records

Declaration of Commitment to Confidentiality for Internal and External Staff

Data protection:

The data protection laws stipulate that personal data be processed in a manner that ensures the rights of confidentiality and integrity of the persons whose data are processed. It is inadmissible to process personal data without authorisation or unlawfully or to violate the security of the processing intentionally or unintentionally in a way that leads to destruction, loss, alteration, unauthorised disclosure or unauthorised access.

In the context of your activity for us, you will gain access to or knowledge of personal data, e.g., about colleagues, customers and other people. You may process personal data only to the extent and in the manner necessary to perform the tasks assigned to you.

Breaches of data protection regulations may result in penalties, fines or imprisonment. If the data subject suffers material or immaterial damage as a result of the unauthorised processing of their personal data, a claim for damages may arise.

A breach of confidentiality and data protection regulations constitutes a breach of employment contract obligations, which can be punished accordingly.

Secrecy and privacy of telecommunications ("Fernmeldegeheimnis"):

If you encounter communication data within the scope of your tasks (e.g., managing email accounts on an administrative level, processing internet communication data, looking after telephone systems or IT network technology, etc.), the so-called "secrecy of telecommunications" (= privacy of telecommunications) also regularly applies. This means that it is prohibited to obtain knowledge of the content or the detailed circumstances of telecommunications beyond what is necessary, as well as it is prohibited to pass on such knowledge to third parties.

If you are looking for further information on data protection, please contact your contact person at the company you are working for if you are an external employee. As an internal employee, you can also find further information on the intranet.

In addition, if you have any questions about the data you process for us, you can contact us via datenschutz@bavaria-film.de.

* For reasons of better readability, the language forms male, female and diverse are not used simultaneously. All references to persons apply equally to all genders.

Declaration of Commitment:

In view of your tasks and with reference to the above explanations, we hereby commit you

- to comply with data protection laws, in particular, not to process personal data without a legal permission,
- to safeguard confidentiality of personal data pursuant to Art. 5 para. 1 lit. f) and Art. 32 GDPR, to which you gain access or of which you obtain knowledge during your activity,
- to observe the secrecy and privacy of telecommunications, as far as relevant to you.

Important: This obligation continues even after your activity has ended!

You will receive the following documents for your records:

- Annex 1: Data protection information sheet
- Annex 2: Selection of legal regulations from GDRP and BDSG

Annex 1 to the Commitment to Confidentiality

Data Protection Information Sheet

When processing personal data, in addition to other laws and regulations, the provisions of the European General Data Protection Regulation (GDPR) and the Federal Data Protection Act ("Bundesdatenschutzgesetz", *BDSG*) are to be observed. The purpose of data protection is to protect individuals from having their personal rights infringed by the processing of their personal data. Responsible processing of personal data is therefore crucial; misconduct can lead to major material and immaterial damage with sometimes considerable negative effects on the part of customers.

The following is an overview of important key statements from the GDPR and the BDSG:

Difference between data protection and data security: Data protection does not protect data as such - the term is incorrect in this respect. Rather, it is about *protecting people* from not being unduly tracked and pictured by third parties. The background to this is personal rights of any person, on the basis of which data relating to a person can always be assigned to that person and in a certain way "depict" that person. For this, there are limits that regulate how much one may process data about a person - these are the data protection laws.
Data security, on the other hand, is purely concerned with the data itself and its technical and organisational protection, for example through encryption, a role and authorisation concept, etc.

Personal data (Art. 4 No. 1 GDPR): Data protection only relates to personal data. This means any information relating to an identified or identifiable natural person (hereinafter: "data subject"), such as employees, colleagues, customers, suppliers, etc. Such data include, e.g., address, telephone number, date of birth, photo, salary, holiday plans, behaviour at work, work results. Data without direct personal reference (e.g., without name) can also be personal data if the associated person can at least be identified from them (e.g., personnel number, PC user ID, etc.). An identifiable natural person is one 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, mental, economic, cultural or social identity of that natural person.

Principle of prohibition and purpose limitation (Art. 5, Art. 6 GDPR): According to data protection law, the processing of personal data is generally prohibited unless the planned data processing is exceptionally permitted by law or the data subject has consented to it. Before processing data, it must therefore be checked whether such an exception exists, as well as whether all possible legal obligations associated with it are complied with, such as the duty to provide information. As a rule, data may only be processed for the purpose for which they were collected; any change of purpose must be permitted.

Breakdown of a processing operation: If data processing consists of several steps (data entry, data transfer, use of data for purpose 1, for purpose 2, etc.), each individual step must be considered individually and checked for a possible processing authorisation and any accompanying obligations.

So-called special categories of personal data (Art. 9 GDPR): Certain types of personal data (often referred to as sensitive data) may as a rule only be collected and processed based on the data subject's consent. This includes data about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning sex life or criminal convictions. In other respects, too, special regulations often apply to this data. Only in a few special cases does permission exist by law for the processing of these data.

* For reasons of better readability, the language forms male, female and diverse are not used simultaneously. All references to persons apply equally to all genders.

Rights of data subjects (Art. 12 et seq. GDPR): Anyone whose personal data are processed has various rights vis-à-vis the data controller, such as the right of access to the personal data and information, e.g. about the purpose of the processing and recipients of transmissions. The data controller must correct any inaccurate data and erase data that are unlawfully stored or are no longer required. If a person suffers damage as a result of unlawful automated processing of their personal data, they must be granted compensation.

Data security by technical and organisational measures (Art. 25, Art. 32 GDPR): The law requires the implementation of appropriate technical and organisational measures necessary to ensure compliance with the provisions of the data protection laws. It is specified that the technology used to process personal data must be designed from the outset in such a way that the data protection principles are effective ("privacy by design"). This also includes the obligation to design and “preset“ the technology and business processes from the outset in such a way that the requirements are met (“privacy by default”).

Notification processes in the event of breaches (Art. 33 GDPR): In the event of a breach of personal data, we as a company may be subject to very strict notification obligations to the supervisory authorities. It is therefore extremely important that every employee who learns of such a breach of data protection immediately reports it to the data protection manager and/or the data protection officer so that they can check what the next steps are.
Attention: We have defined a process for this in the form of a data protection guideline that must be adhered to. You can find this guideline on the intranet or obtain it from our data protection manager.

Each individual employee is responsible for complying with data protection requirements. Correct behaviour is therefore indispensable.

If you have any questions about data protection or data security or in cases of doubt, please contact – better too often than too little – us via datenschutz@bavaria-film.de.

* For reasons of better readability, the language forms male, female and diverse are not used simultaneously. All references to persons apply equally to all genders.

Annex 2 to the Commitment to Confidentiality

Copy of selected Statutory Provisions from the GDPR (EU General Data Protection Regulation) and German BDSG (Federal Data Protection Act) (no official translations)

This selection of statutory provisions is intended to give you an overview of the data protection regulations. The presentation is exemplary and by no means complete. Further information on data protection issues can be obtained from the corporate data protection officer.

Definitions

Art. 4 Nr. 1 GDPR: **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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, mental, economic, cultural or social identity of that natural person.

Art. 4 Nr. 2 GDPR: **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Principles relating to processing of personal data

Art. 5 (1) lit. a) GDPR: Personal data shall be (…) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

Art. 5 (1) lit. f) GDPR: Personal data shall be (…) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Art. 29 GDPR: The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Art. 32 para. 2 GDPR: In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Art. 33 para. 1 sentence 1 GDPR: In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent (…), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Liability and penalties

Art. 82 para. 1 GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

* For reasons of better readability, the language forms male, female and diverse are not used simultaneously. All references to persons apply equally to all genders.

Art 83 para. 1 GDPR: Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation (…) shall in each individual case be effective, proportionate and dissuasive.

§ 42 BDSG

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:
1. transferring the data to a third party or
2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. Processing without authorization, or
2. Fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

§ 202a para. 1 StGB (Strafgesetzbuch; German Penal Code): Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

§ 303a para. 1 StGB (Strafgesetzbuch; German Penal Code): Whosoever unlawfully deletes, suppresses, renders unusable or alters data (…) shall be liable to imprisonment not exceeding two years or a fine.

Privacy of Telecommunications (if applicable)

§ 3 TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz; Telecommunications Telemedia Data Protection Act)

(1) The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts.

(2) The following are obliged to maintain telecommunications secrecy

1. Providers of publicly available telecommunications services as well as natural and legal persons involved in the provision of such services,
2. providers of telecommunications services offered wholly or partly on a commercial basis as well as natural and legal persons involved in the provision of such services,
3. operators of public telecommunications networks, and
4. operators of telecommunications installations with which telecommunications services are provided on a business basis.

The duty of confidentiality shall continue to exist after the end of the activity by which it was established.

(3) All persons with obligations according to subsection (2) shall be prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems. Knowledge of facts which are subject to telecommunications privacy may be used solely for the purpose referred to in sentence 1. Use of such knowledge for other purposes, in particular, passing it on to other parties, shall be permitted only insofar as provided for by this Act or any other provision and reference is made expressly to telecommunications activities. The reporting requirement according to section 138 of the Penal Code shall have priority. (…)