Code of confidentiality under GDPR for freelancers

As a company, we are legally obliged to process personal data in such a way as to safeguard the rights of the data subjects and to guarantee the confidentiality and integrity of their data[1]. You may therefore only process personal data to the extent and in the manner required to perform the tasks assigned to you.

You are prohibited under this code to process personal data unlawfully or without authorisation or to intentionally or unintentionally compromise the security of the processing in a way which results in destruction, loss, alteration, unauthorised disclosure or unauthorised access.

Infringements of the data protection regulations may be punished by fines, penalties or imprisonment. Data subjects who suffer material or immaterial damage as a result of the unauthorised processing of their personal data may be able to claim damages.

A breach of confidentiality standards and data protection regulations shall constitute a breach of contractual obligations and may be punished accordingly.

The undertaking to observe confidentiality shall continue to apply after the end of the contractual relationship.

_____[*Name of freelancer*] hereby issues _____[*Name of commissioning Burda company*] with the required confirmation, duly undertaking to comply with the applicable data protection regulations in respect of the confidentiality and integrity of personal data.

By signing you also confirm receipt of a copy of this document and any appendices.

_____, _____ _____

Place Date Signature of Declarant

Appendices:

1. Summary of the main provisions of data protection law
2. Technical and organisational measures

[1] Should your job involve secrecy of telecommunications, confidentiality of social security data, client confidentiality in legal matters or patient confidentiality, you are obliged to comply with further legal requirements over and above the General Data Protection Regulation and the other general provisions of data protection law.

Summary of the main provisions of data protection law

Appendix 1 to the code of confidentiality for freelancers

The passages selected below are intended to provide an overview of the main data protection regulations. The paragraphs are cited as examples and the notes are by no means exhaustive. Further information on data protection issues can be obtained from the company data protection officer.

Article 4 General Data Protection Act ("GDPR") – Definitions

For the purposes of this Regulation:

(1) '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;

(2) '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;

Article 5 GDPR – Principles relating to processing of personal data

1. Personal data shall mean:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   (f) 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').

Article 29 GDPR – Processing under the authority of the controller or processor

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.

Article 32 GDPR – Security of processing

2. 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.

Article 33 GDPR – Notification of a personal data breach to the supervisory authority

1. 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 in accordance with Article 55, unless the

personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Article 82 GDPR – Right to compensation and liability

1. 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.

Article 83 GDPR – General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

Section 42 Bundesdatenschutzgesetz (Federal Data Protection Act) – Penal provisions

(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 Strafgesetzbuch ("StGB", German Criminal Code) – Data espionage

(1) 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 StGB – Data tampering

(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.

Technical and organisational measures

Appendix 2 to the code of confidentiality for freelancers

Hubert Burda Media ("**HBM**") puts appropriate technical and organisational measures in place to ensure the protection of personal data and the confidentiality of information. The more sensitive the data to which the freelancer[1] has access, the more carefully they must be protected. The following general conditions apply:

1. Use of HBM IT systems

The following rules apply to the use of HBM IT systems:

a) Do not make any changes to the security settings
b) Do not use any hardware and software other than that which has been approved in advance by the iSecurity department and by HBM data protection staff (e.g. apps)
c) Do not use any USB sticks other than those provided by HBM (the use of USB disk drives is not permitted)
d) Do not use any cloud services which have not been approved by the Information Security Officer ("**ISO**") of the commissioning HBM company or by the Chief Information Security Officer ("**CISO**") of HBM
e) Do not provide or access content which infringes data privacy law, personal rights, copyright or penal law provisions
f) Do not share content publicly in digital form (e.g. newsletters) except by agreement with the internal contact person at HBM
g) Use a secure password to protect IT systems and data from third-party access and do not share this password
h) Arrange for accounts which are used for company business and which are supplied by providers like Apple, Amazon or Google to be managed from a central location in the company
i) Do not use private accounts for business purposes; do not open private accounts in the email programs provided (e.g. Outlook)
j) Do not use cloud services other than those provided by HBM for the storage of HBM data
k) Do not use internal applications on mobile IT systems except over high-security network connections
l) Erase personal data on termination of the collaboration and hand over company data to the relevant contact person at HBM (including passwords for external services which were used professionally) or erase the data by arrangement

2. Use of own IT systems

If the freelancer uses his own IT systems, he must be able to demonstrate to the ISO of the commissioning HBM company or to the CISO that he has put such technical and organisational measures in place to protect personal data and to safeguard the confidentiality of information in any given case as are appropriate and as provide equivalent levels of protection to the measures listed in section 1.

[1] The masculine form is used in case of personal references below. All such references refer to both males and females.