DEval
GERMAN INSTITUTE FOR DEVELOPMENT EVALUATION

ENCLOSURE 4

Declaration of Commitment to Safeguarding the Confidentiality of Personal Data

---

German Institute for Development

Evaluation (DEval)

Fritz-Schäffer-Str. 26, 53113 Bonn, Germany

- Customer -

and

- Contractor -

In consequence of having been awarded a contract by us, you are subject to the provisions of data protection law. The following notice therefore binds you to data secrecy and advises you of the criminal penalties for infringements.

You are prohibited from processing personal data to which you might have access in the course of your work for any purposes other than those relating to the legitimate performance of your given duties, without due authorisation.

The commitment to data secrecy remains in force without time limitation and continues after your work with us has ended.

The points covered particularly – but by no means exhaustively – by the commitment are the following:

- All data and programs must be stored, processed or distributed only in the way directed by bodies authorised to make such decisions.
- Data, programs and other information must not be reproduced for any purpose other than the business purpose.

- It is prohibited to falsify data or programs, to produce counterfeit data or programs, or intentionally to make use of counterfeit or falsified data or programs.
- It is only permissible to retrieve the data necessary for the performance of the specific duties.
- Transfer of personal data to third parties is only permissible if the recipient has a right, on the grounds of a legal regulation, to gain access to such data.
- Documents containing personal data are to be kept safe from access by third parties.
- Data media or printouts intended for deletion or destruction are to be deleted or destroyed in the proper manner.
- Trade secrets within the meaning of Section 2 No. 1 of the German Act on the Protection of Trade Secrets (Gesetz zum Schutz von Geschäftsgeheimnissen, GeschGehG) and information subject to banking secrecy that come to your knowledge in the course of your work must be treated as strictly confidential and may only be used for the contractually agreed purposes.
- If you use artificial intelligence in your work, you have an obligation to inform DEval of this and to disclose and document the applications used and the extent of your use of AI. Only AI applications that guarantee an appropriate level of data protection and data security may be used in the processing of non-public, confidential or personal data (cf. section 1.11 of the DEval General Terms and Conditions of Contract).

The Contractor is informed that infringements of data secrecy can be punished according to Sections 42 and 43 of the Federal Data Protection Act (BDSG) and other relevant legal regulations (see Annex) with imprisonment or fines.

Please provide your signature to confirm that you acknowledge the commitment to data secrecy and recognise it as an integral part of the main contract concluded with you.

Other confidentiality obligations under other regulations shall not be affected by this commitment.

_____ _____

Place, Date Signature

Annex to the Commitment to Confidentiality (as of May 2018)

It is important that personal data are protected within DEval. You will also have to handle **personal data** in some form as a result of having been awarded a contract by us.

The **General Data Protection Regulation (GDPR)** obliges our company, and also you, to ensure the careful and lawful handling of any information that can be associated directly or indirectly with a natural person.

"The purpose of data protection is to prevent any impairment of the individual's right to privacy resulting from the handling of his or her personal data."

Be mindful of the data protection regulations in your daily work. Please treat the personal data that you process in the course of your duties just as carefully as you would wish your own data to be handled.

What are personal data within the meaning of the GDPR?

'Personal data' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name (Art. 4 (1) GDPR).

Examples of personal data are: name, address, date of birth, telephone number, or details about residential or financial circumstances, as well as IP addresses.

Principles for the processing of personal data

'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 (Art. 4 (2) GDPR).

Principle of lawfulness

Personal data may only be processed if this is lawful. Data processing is only lawful if it is permitted by the GDPR itself or by another legal regulation, or if the data subject has given consent to the processing of his or her personal data.

The data processing that is necessary to fulfil contractually regulated business purposes is permitted by the provisions of the GDPR.

The data subject's consent constitutes an authorisation pursuant to the GDPR. It must normally be given in writing and can be withdrawn at any time. It is only valid if the subject was provided with sufficient information beforehand and the consent was given voluntarily.

Responsibility for data processing

According to the GDPR, any person or body that make decisions about the purposes and means of processing of personal data is responsible for compliance with data protection.

You, as a contractor processing personal data in the course of your work, are likewise responsible for compliance with the data protection regulations.

General principles for the processing of personal data

According to the principle of data avoidance and economy, as far as possible the processing of personal data is be avoided or, if this is not possible, done using the fewest possible items of data.

Furthermore, every data subject is to be informed about the processing of his or her personal data and has the right to obtain information about who is processing which of his or her data for what purpose.

In this way personal data are to be protected from manipulation and misuse and processed in a transparent way.

The processing of personal data itself is to be carried out with due regard to the aspect of necessity. Technical and organisational measures for the protection of personal data are to be taken likewise, insofar as the expenditure involved is in reasonable proportion to the purpose of protection.

The above selection is intended to give you an overview of the data protection legislation, but is by no means complete. Further information on questions arising under data protection law can be obtained from your corporate data protection officer.

Appended are excerpts of relevant legislative provisions on sanctions and penalties:

German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb, UWG)
Section 17 Betrayal of business and corporate secrets

(1) Whosoever as a person employed by a company communicates, without authorisation, a business or corporate secret that was entrusted or made accessible to him or her during the term of the employment relationship to another person for purposes of competition, for personal gain, for the benefit of a third party or with the intention of harming the owner of the company, shall be punished with imprisonment of up to three years or a fine.

(2) Likewise, whosoever for purposes of competition, for personal gain, for the benefit of a third party or with the intention of harming the owner of the company,

1. without authorisation, obtains or secures a business or corporate secret by

    a) making use of technical means,

    b) producing an embodied reproduction of the secret, or

    c) removing an item in which the secret is embodied,

or

2. without authorisation, exploits or communicates to anyone a business or corporate secret to which he gained access by means of one of the transactions described in subsection (1) or through action taken by himself or a third party under number 1. or which he otherwise obtained or secured without authorisation

shall be subject to the same punishment.

(3) The attempt shall be punishable.

(4) In especially serious cases the punishment shall be imprisonment of up to five years or a fine. In general a case shall be especially serious if the perpetrator

1. acts for commercial purposes,

2. knows at the time of the communication that the secret will be exploited abroad, or

3. take steps himself to exploit it abroad according to subsection (2) number 2.

(5) The offence shall be prosecuted only if a complaint is filed unless the criminal prosecution authorities consider it imperative to intervene ex officio due to the particular public interest in criminal prosecution.

(6) Section 5 number 7 of the Criminal Code shall apply mutatis mutandis.

German Criminal Code (Strafgesetzbuch, StGB)
Section 202a Data espionage

(1) Whosoever, without authorisation, accesses data for himself or another which are not intended for him and are especially protected from unauthorised access, by overcoming the access protection, shall be punished with imprisonment of up to three years or a fine.

(2) Data within the meaning of subsection (1) shall only be those which are stored or transmitted by electronic, magnetic or other not directly perceivable means.

Section 263a StGB Computer fraud

(1) Whosoever, with the intention of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of the program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the process, shall be punished with imprisonment of up to five years or a fine.

(2) Section 263 subsections (2) to (7) shall apply mutatis mutandis.

(3) Whosoever makes preparations for an offence under subsection 1 by writing, obtaining for himself or another party, offering for sale, storing, or supplying to another party computer programs, the purpose of which is to commit such an act, shall be punished with imprisonment of up to three years or a fine.

(4) In the cases under subsection (3), Section 149 subsections (2) and (3) shall apply mutatis mutandis.

Section 303a StGB Alteration of data

(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (Section 202a subsection (2)) shall be punished with imprisonment of up to two years or a fine.

(2) The attempt shall be punishable.

(3) For the preparation of an offence under subsection (1), Section 202c shall apply mutatis mutandis.

German Act on Copyright and Related Rights (Urheberrechtsgesetz, UrhG)
Section 106 Unlawful exploitation of works protected by copyright

(1) Whosoever without the consent of the rights-holder reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, in cases other than those permitted by law, shall be punished with imprisonment of up to three years or a fine.

(2) The attempt shall be punishable.

EU General Data Protection Regulation (GDPR)
Art. 82 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.

(2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(3) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

(6) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

New German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG-neu)
Section 42

(1) The following actions done deliberately and without authorisation 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 authorisation, or
2. fraudulently acquiring

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

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal proceedings against the person required to provide a notification or a communication, or his or her relatives as referred to in Section 52 (1) of the Code of Criminal Procedure, only with the consent of the person required to provide a notification or a communication.

Section 43 BDSG-neu
Provisions on administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offence:

1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

(3) Authorities and other public bodies as referred to in Section 2 (1) shall not be subject to any administrative fines.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication, or his or her relatives as referred to in Section 52 (1) of the Code of Criminal Procedure, only with the consent of the person required to provide a notification or a communication.