DIW BERLIN

**Statement on Upholding Data Secrecy and Security**

I, _____, hereby declare

that I have been informed today about the relevant provisions of the European General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG), the resulting special requirements for data security and data protection using micro-data of the SOEP in the DIW Berlin and that I am obliged to comply with these legal data protection regulations.

According to these regulations, personal data must be processed in such a way that the rights of data subjects to the confidentiality and integrity of their data are not affected. Therefore, personal data may only be processed to the extent and in the manner necessary to perform the tasks assigned to me.

According to legal regulations, it is prohibited to process personal data without authorization or unlawfully, or to violate the security of the processing in a way that leads to the destruction, loss, alteration, or unauthorized disclosure or access to the data. Furthermore, personal data must be treated confidentially and may not be passed on to third parties without authorization. Documents containing personal data must be stored in such a way that they are protected from being accessed by third parties.

I am aware that any measures of de-anonymization are not permitted, that the publication of individual datasets and merging of the data with other non-anonymized SOEP data is strictly prohibited.

I am also aware that breaches of data protection legislation can be punishable by fines, penalties, or imprisonment. It may also give rise to claims for damages on the part of the persons concerned.

_____

(Location, date, signature)

**Appendix to the Statement on Upholding Data Secrecy and Security**

This selection of legal excerpts is intended to give you an overview of the data protection regulations. The selection contains examples and is by no means complete. Further information on data protection issues can be obtained from DIW Berlin's data protection officer.

**Definitions**

**Article 4, number 1 of the 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.

**Article 4, number 2 of the 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, organization, 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 the processing of personal data**

**Article 5, paragraph 1, point a of the GDPR**: Personal data shall be [...] processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness, and transparency").

**Article 5, paragraph 1, point f of the GDPR**: Personal data shall be [...] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")

**Article 29 of the 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.

**Article 32, paragraph 2 of the 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, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

**Article 33, paragraph 1, sentence 1 of the 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 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.

**Liabilities**

**Article 82, paragraph 1 of the 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.

**Article 83, paragraph 1 of the 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.

**Section 42 of the 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.

**Section 202a, paragraph 1 of the StGB**: Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

**Section 303a, paragraph 1 of the StGB**: Whoever unlawfully deletes, suppresses, renders unusable or alters data [...], shall be punished with imprisonment for not more than two years or a fine.

Last updated: May 2018