|  |
| --- |
|  |

First name and family name of the intern

|  |
| --- |
|  |

Organizational unit/institute contact person

**Information on Compliance with Data Secrecy**

|  |
| --- |
| Dear |

This is to inform you about your obligation to comply with data secrecy (Article 3, par. 2, Landesdatenschutzgesetz – LDSG (State Data Protection Act)). In case you are involved in rendering business-related telecommunications services during your work (e.g. writing of emails), you are also obliged to observe secrecy of telecommunications (Article 88, Telekommunikationsgesetz – TKG (Telecommunications Act)).

These obligations continue to apply even after termination of your work at Karlsruhe Institute of Technology.

In detail, this means:

You are not allowed to process or use personal data in an unauthorized manner. You are only allowed to store, modify, transmit to third persons, or use personal data of colleagues and other external partners to the extent required for company purposes, provided that this is in agreement with data protection regulations. In addition, you are obliged not to disclose any information obtained during your work on circumstances and contents of personal documents.

Violations of data secrecy or other data protection regulations, in particular unauthorized data processing or fraudulent use of legally protected data, may be punished by a fine or imprisonment according to Article 84 Datenschutzgrundverordnung-DS-GVO (General Data Protection Regulations (GDPR)) in conjunction with Article 29, par. 1, LDSG.

By signing this document, you confirm that you have been informed about data secrecy. **I have been informed about the legal obligation to comply with data secrecy. In addition, I have been informed about the resulting practices.**

**PSE\_PRAK\_Wahrung-Datengeheimnisses\_EN\_2024-03-13**

|  |  |  |
| --- | --- | --- |
|  |  |  |

Date Intern’s Signature

Annex:

* Article 4, GDPR [Excerpt] “Personal Data“
* Article 3, LDSG “Ensuring Data Protection“
* Article 29, LDSG “Penal Provisions“

**Article 4, No. 1 General Data Protection Regulation [Excerpt]**

According to this regulation,

|  |  |
| --- | --- |
| No. 1 | “personal data“ are all data referring to an identified or identifiable natural person (hereinafter called “data subject”); an identifiable natural person is a natural person that can be identified directly or indirectly by allocation to an identifier, such as a name, an identification number, location data, an online code, or one or several special characteristics reflecting the physical, physiological, genetic, psychic, economic, cultural, or social identity of this natural person.  […] |

**Article 3, LDSG Ensuring Data Protection**

(1) 1When processing data, adequate and specific measures must be taken to protect the interests of the data subject.  2For this, the state of the art, implementation costs, the type, scope, circumstances, and purposes of processing, and variable probability of occurrence and seriousness of the risks to the rights and freedoms of natural persons, which are associated with processing, must be taken into account. 3Such measures may include:

|  |  |  |
| --- | --- | --- |
|  | 1. | Technical and organizational measures to ensure that processing takes place in agreement with Directive [EU] 2016/679, |
|  | 2. | measures ensuring subsequent verification and assessment whether and by whom personal data were collected, changed or deleted, |
|  | 3. | sensitization and training of persons involved in processing, |
|  | 4. | restriction of access to personal data at the public office and for processors, |
|  | 5. | pseudonymization of personal data, |
|  | 6. | encryption of personal data, |
|  | 7. | the ability to permanently ensure confidentiality, integrity, availability, and resilience of systems and services in connection with the processing of personal data, including the ability to quickly restore the availability of personal data and access to them in case of a physical or technical incident, |
|  | 8. | establishment of a procedure for the regular check, assessment, and evaluation of the effectiveness of technical and organizational measures to ensure safety of processing, and |
|  | 9. | specific procedures ensuring compliance with the requirements of this act and of Directive [EU] 2016/679 in the case of transmission or processing of personal data for other purposes. |

(2) 1Persons employed at public offices are not allowed to process personal data unauthorized (data secrecy). 2The data secrecy obligation shall remain effective even after termination of their activity.

**Article 29, LDSG Penal Provisions (to complement Article 84 of the Directive [EU] 2016/679)**

(1) Persons shall be punished by imprisonment for up to two years or a fine, if they

|  |  |  |  |
| --- | --- | --- | --- |
|  | 1. | a) | store, use, change, transmit or delete protected personal data, |
|  |  | b) | keep available protected personal data for retrieval by an automatic process, or |
|  |  | c) | retrieve protected personal data or obtain access to them in files for themselves or others |
|  |  | without being authorized by this Act or Directive (EU) 679/2016, or if they | |
|  | 2. | fraudulently obtain by the provision of incorrect information personal data that are protected by this Act or Directive (EU) 679/2016 and are not generally accessible | |

against payment or with the intention to enrich themselves or others or to damage another person.

(2) 1The act will be prosecuted on request only.  2This request may be made by the data subject, public office, processor, State Data Protection Commissioner, Radio Officer for Data Protection, and supervisory authorities.

U\_PSE\_PB\_PRAK-CN\_01\_05-20 Vorübergehend