**E. 2. Verpflichtung auf die Vertraulichkeit für Mitarbeiter**

**Verpflichtung auf die Vertraulichkeit**

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet

werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist. Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann. Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses

fort.

Name des Mitarbeiters:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten. Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Verpflichtete(r)

**Anlage zur Verpflichtung auf die Vertraulichkeit**

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

**Begrifflichkeiten**

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**Grundsätze der Verarbeitung**

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] auf **rechtmäßige Weise**, nach

Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich** **auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die

Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind. Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die **Verletzung** bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

**Haftung**

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einemanderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

**Obligation of confidentiality**

The relevant legal provisions require that personal data be processed in such a way that that the rights of data subjects to confidentiality and integrity of their data are guaranteed. Therefore, you are only permitted to process personal data to the extent and in the manner necessary to fulfil the tasks assigned to you. These rules prohibit unauthorised or unlawful processing of personal data or intentionally or unintentionally breaching the security of processing in a way that leads to destruction, loss, alteration, unauthorised disclosure or unauthorised access.

Violations of data protection rules may be punishable by a fine, a financial penalty or imprisonment. If the data subject suffers material or non-material damage as a result of the unlawful processing of his or her personal data, he or she may be entitled to compensation.

A breach of confidentiality and data protection regulations constitutes a breach of obligations under employment contracts, which may be punished accordingly. The obligation of confidentiality remains in force even after the termination of the employment relationship gone.

Name of the employee:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

declares to comply with the requirements of the applicable data protection legislation as regards the confidentiality and integrity of personal data. With your signature, you also confirm receipt of a copy of these minutes and their annex.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place, date Obligated party

**Annex on the confidentiality obligation**

This selection of legal regulations 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 company data protection officer.

**Terminology**

Art. 4 No. 1 GDPR: "Personal data" means any information relating to an identified or identifiable natural person (hereinafter "data subject"); as identifiable means any natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, a location data, an on-line identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Art. 4 No. 2 GDPR: "processing" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Principles of processing**

Article 5 (1) lit. a GDPR: Personal data must be [...] processed lawfully, in accordance with processed fairly and in a way that is comprehensible to the data subject ("lawfulness, fairness, transparency").

Article 5 (1) lit. f GDPR: Personal data must [...] be processed in a way that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, accidental destruction or accidental harm by appropriate technical and organisational measures ("integrity and confidentiality").

Art. 29 GDPR: The processor and any person under the authority of the controller or the processor who has access to personal data may process such data only on instructions from the controller, except where they are obliged to do so by Union or national law.

Article 32(2) GDPR: In assessing the adequate level of protection, particular attention shall be paid to to take account of risks linked to the processing, in particular by destruction, loss or alteration, whether accidental or unlawful, or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. Article 33 (1) sentence 1 DS-GVO: In the event of a violation of the protection of personal data, the controller shall notify the competent supervisory authority [...] without delay and, if possible, within 72 hours of becoming aware of the violation, unless the violation of the protection of personal data is not likely to jeopardise the rights and freedoms of natural persons.

**Liability**

Art. 82 (1) GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall be entitled to damages against the person responsible or the processor. Art. 83 (1) DS-GVO: Each supervisory authority shall ensure that the imposition of fines pursuant to this Article for infringements of this Regulation [...] is effective, proportionate and dissuasive in each individual case.

§ 202a (1) StGB: Whoever gains unauthorized access to data which is not intended for him or her or to data which is specially secured against unauthorized access, while overcoming the access security, shall be punished with imprisonment for up to three years or with a fine.

§ 303a StGB: Whoever unlawfully deletes, suppresses, makes unusable or alters data [...] will be punished with imprisonment for up to two years or with a fine.