

**Exhibit 1**  
**To the General Works Agreement on the Limited Private Use of IT Systems**

**Declaration of Consent regarding the collection, processing and usage of personal data**

(This declaration is voluntary and without influence on the employment relationship)

1. Microsoft Deutschland GmbH permits the merely occasional private and non-commercial use of the IT systems which are provided for business purposes subject to the condition that I submit the declaration of consent specified below. The availability of the IT systems may not be compromised by the private use.

2. No distinction between business and private use shall be made by technical means. Thus, data generated by the system will be logged and stored to ensure due operation of the IT systems, for security reasons and control of abuse, respectively. The standards set for the business use apply. I am aware that Microsoft Deutschland GmbH uses the IT systems provided by Microsoft Corporation and therefore all logging and storage takes also place at the registered office of Microsoft Corporation in Redmond, USA.

The following data shall be logged and stored:

**Internet usage:**

- Access to the Internet server including the URL of the selected site
- IP address of the PC used to access the internet
- Date and time of the activity
- The name of the account used to access the internet
- The name of the application used to access the internet

**Email usage:**

- Sender's email address
- Recipient's email address
- Date and time of activity
- Subject line of the e-mail
- Additional technical details relating to the delivery and routing of email

To warrant the due course of business, ITG shall make backups of the Exchange Servers for security purposes.

**Corporate Network:**

Automatic scanning mechanisms may be used to ensure the security of the entire network. Such scanning procedure shall be carried out in specific temporal intervals without reference to particular users in order to discover patterns of suspicious activities (unauthorized access, viruses, illegal activities).

Furthermore, the log-in information of each user may be stored and reviewed to prevent unauthorized access to the network.

**With the submission of this declaration of consent I hereby explicitly agree to the activities of Microsoft listed above.**

3. The works council agreement about the permission for the limited private use of IT systems governs the requirements and scope for the use of data as well as for the collection and processing of data. These requirements in particular provide that the data are not used to control the conduct and performance, unless there are justified reasons for the suspected and severe violation of the codes of conduct mentioned below.

4. As for the rest, the following limitations of use shall apply:

The occasional private use of the IT systems is permitted provided neither the fulfillment of responsibilities nor company interests and processes are impaired and provided they do not conflict with corporate interests.

The use of data for private commercial purposes shall be prohibited in any case.

The employer shall not warrant any liability for the operability of the IT systems.

Access, storage and transmission of files containing content regularly perceived as repugnant and/or content violating the rights of third parties (such as pornographic and racist content, content glorifying violence or violating human dignity, or extremist or any other criminally liable content) shall be prohibited.

5. I am aware that no technical differentiation is made between the business and private use of the IT systems. This means in particular that my business email account may also be viewed by third parties in justified cases. This shall in particular apply to – but not exclusively – to the substitutes during my absence. I am aware that confidentiality of private emails cannot be warranted as a consequence.

**With the submission of this declaration of consent I hereby explicitly agree to it.**

6. It is herewith clarified that permission according to paragraph 1 does not justify any legal claim (in time and content) for the use of the corporate IT system, for additional services and technical support for private purposes. Permission for the private use of the IT systems can therefore be revoked by Microsoft Deutschland GmbH.

7. Upon my agreement on these principles, they shall take effect immediately. I am able to revoke this declaration of consent at any time in the future in writing without causing any impact on the employment contract. As a result, permission for the private use of the IT systems shall cease at the same time.

8. If I do not agree on these principles, or if I do not submit any statement, the use of the IT systems provided by Microsoft shall be admissible for business purposes only. **Any private use shall be fully prohibited without a valid declaration of consent.** Violation against such prohibition may result in consequences relating to labor law (letter of warning, termination of contract). I am able to provide my consent to the aforementioned principles retrospectively at any time by signing this declaration.

I am aware of the fact that the prohibition of the private use will be randomly checked by the Corporation. Control is performed in coordination with the responsible works council.

9. I have read and understood the aforementioned principles of Microsoft Deutschland GmbH about the private use of IT systems.

**I agree on these principles:**

Date: 5/24/2023

Employee: Lixue Cheng

Signature: \_\_\_\_\_

DocuSigned by:

*Lixue Cheng*

948642555631489...



Lixue Cheng

Name, Vorname

**A. Duty of confidentiality under data protection law and declaration of obligation****Duty to maintain confidentiality**

Dear Employee,

Within the scope of your employment you have access to personal data which you process or else are involved with processing. You are consequently obliged to:

- treat personal data confidentially,
- process personal data exclusively for the purposes for which they have been entrusted to you within the scope of your employment.
- desist from engaging in unauthorised attempts to access applications or data,
- ensure that data you use for accessing data processing systems are not used by other persons,
- comply with relevant existing guidelines, policies and regulations governing the handling of personal data, as well as with IT security.

The obligation to maintain confidentiality shall also extend beyond the termination of your employment at our company.

In the event of any breach of duties arising from this obligation, we reserve the right to take necessary legal action under labour law.

We call your attention to the fact that violations against data protection regulations may also render you personally liable to a fine or imprisonment. A collation of the most pertinent provisions is attached to this notification.

This declaration is without prejudice to your general duty of confidentiality arising from the employment/service contract and from relevant existing guidelines, policies and regulations, where applicable.

**Declaration of obligation**

I have been informed of the statutory provisions of the EU General Data Protection Regulation and of the German Federal Data Protection Act (2017). I will undertake to observe confidentiality and to process personal data exclusively in accordance with the controller's instructions.

Berlin

5/24/2023

DocuSigned by:

948642555631489...

Place, Date

Signature of Employee

**B. Duty of confidentiality on the part of the Employee**

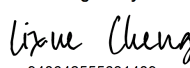
- (1) The Employee is required, both during his/her employment relationship and following its termination, to observe the strictest confidentiality regarding all business and trade secrets of the Employer or of companies affiliated with the Employer ("affiliated companies") within the meaning of §§ 15 et seq. of the German Stock Corporation Law, as well as regarding such issues and matters, information, documents and data sets which are designated by the Employer or an affiliated company as confidential or for internal use or which otherwise are self-evidently confidential, and neither to forward same or in any other way make same available to third parties.

Confidential information includes, in particular, but is not limited to:

- company and marketing strategies, the development of the company, internal reports and statistical material;
  - company methods and processes, manuals and technical information, as well as know-how relating to the corporate group, that is not in the public domain, particularly inventions, designs, programmes, techniques, data-based systems, formulas and ideas;
  - contacts of the company, pricing policy, client names and supplier names, as well as the contents of agreements (both existing and future) entered into with clients and suppliers;
  - information about employees, including their qualifications, as well as details of their employment contracts;
  - budgets, cost information and other reports concerning the company's finances.
- (2) The Employee is obliged to observe the strictest confidentiality regarding all business and trade secrets of clients and business partners of the Employer or of affiliated companies of which he/she becomes aware within the scope of his/her employment for the Employer. The same applies to issues and matters, documents, data sets and computer programmes of clients and business partners of the Employer or of affiliated companies of which the Employee becomes aware within the scope of his/her employment for the Employer and which are designated as confidential or for internal use or which otherwise are self-evidently confidential.
- (3) The Employee shall respect the Employer's general and specific instructions for maintaining confidentiality. In case of doubt, the Employee shall seek instructions from the Employer relating to the confidentiality of specific facts.
- (4) If the post-contractual duty to maintain confidentiality unduly impairs the Employee in his/her further career pursuits, he/she shall be entitled to be released by the Employer from this duty.

Berlin

5/24/2023

DocuSigned by:  
  
 948642555631489...

Place, Date

Signature of Employee

Munich

5/24/2023



Place, Date

Signature of Employer

## Excerpt from the EU General Data Protection Regulation (GDPR)

### Article 5 – Principles relating to processing of personal data

#### (1) Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- 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 – 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 83 – General conditions for imposing administrative fines

- (4) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
  - a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- (5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
  - a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
  - b) the data subjects' rights pursuant to Articles 12 to 22;
  - c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
  - d) any obligations pursuant to Member State law adopted under Chapter IX;
  - e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
- (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

## Excerpt from the Federal Data Protection Act (FDPA 2017)

### § 41 – Application of provisions concerning criminal proceedings and proceedings to impose administrative fines

- (1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. [...]

### § 42 – Penal provisions

- (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 someone else or harming someone.
- (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.



