



## Data Use Agreements

*Ulrich Herfurth, attorney-at-law in Hanover and Brussels*

*July 2024*

As part of the cooperation between the supplier and the customer, it is recommended that a binding regulation be introduced for the processing of data generated during the operation of the machines. This recommendation aims to clearly regulate the use, protection and rights to the data. The basis for the delivery of the machines is a purchase and delivery contract in which the machines are equipped with an electronic control system that is maintained by the supplier as part of a maintenance contract.

### **Collection and transmission of data**

#### *Purpose of the transfer*

The supplier shall provide the customer with the data required for the operation of the machine, including software for controlling and monitoring the machine. Conversely, the customer provides the supplier with data from the operation of the machine so that the supplier can carry out maintenance and testing tasks. This data is also used for analysis to optimise performance and improve machine functions.

#### *Data concerned*

The agreement should stipulate that all data contained in the system when the machine is handed over or generated by the machine after handover fall

within the scope of the agreement. This includes both the data provided by the supplier and the data generated by the operation of the machine. This may include, for example, process data, sensor data or operating logs that are continuously generated during the use of the machine.

It should also be specified which data is not covered by the agreement. This applies in particular to data that the customer or the supplier generates independently of the machine. This data is not related to the operation of the machine and is therefore not subject to the rights of use or property rights defined in the agreement.

An explicit declaration or confirmation of the inclusion of the data concerned by the parties is not required. This data is automatically included in the agreement when the machine is used in order to facilitate the processes and avoid potential uncertainties.

#### *Provision of the data*

The relevant data can be transmitted in different ways. It should be specified that the data can be transmitted to the supplier both digitally via remote access and, if necessary, via physical data carriers. It must also be clarified who is responsible for ensuring the correct transmission and integrity of the data.



## Data rights and rights of use

### *Ownership of data*

The agreement must clearly regulate that the rights to the data generated by the machine belong to the customer. This data constitutes trade secrets of the customer and its use by the supplier should be strictly regulated. In contrast, the data generated by the maintenance and inspection of the machine belongs to both the customer and the supplier, as both parties are dependent on this data to ensure the operation of the machine.

### *Intellectual property and industrial property rights*

As a rule, the data concerned should not be classified as intellectual property unless it contains specific property rights, for example through copyrights to software, databases or technical works. In such cases, the corresponding intellectual property rights should remain unaffected. Both parties should respect the rights to the data assets and only use them within the scope of the agreement. This particularly protects investments in software, database solutions and technical developments.

### *Rights of use to the data*

The agreement should grant each party the right to use the data assigned to them. The supplier is entitled to analyse and evaluate the data generated by the operation of the machine, but only on condition that this data is anonymised and cannot be traced back to the customer. This serves to protect the customer's operational confidentiality.

The parties must then clarify the scope of authorised data use:

- Earmarking of the utilisation
- Processing and merging of data sets
- Analysing the data provided
- Analysis and utilisation of merged data

- Utilisation of data from processing operations involving the data provided
- Analysing data sets from data provided by the transferor
- Analysing datasets from data provided by the transferor and from other sources
- The transferor's right to the results of the transferee's analyses
- Passing on data sets in the service chain to authorised processors
- Conditions for transfer
- Disclosure to third parties
- Evidence of data handling in escrow
- Control rights of the transferor at the recipient
- Use as training data for AI

### *Analysing the machine and system data*

The supplier should be given permission to analyse the data generated by the operation of the machine. The aim is to use these analyses to draw conclusions about the machine's performance and identify optimisation opportunities. Such analyses can help the customer to make operation more efficient and identify any faults or potential for improvement at an early stage.

### *Further use of data and analyses*

The supplier may use the analysis results for its own purposes but may only pass them on to third parties if the origin of the data is anonymised and does not allow any conclusions to be drawn about the customer. This enables the supplier to use the knowledge gained for the further development of its products or services, for example, without breaching confidentiality obligations.

### *Responsibility for incorrect analyses*

It is important to define liability rules in the event of incorrect data analyses. The supplier should not be



liable for unforeseeable errors or incorrect analyses unless these are due to gross negligence or wilful misconduct. This creates a clear basis for liability and minimises risks for both parties.

### *Data as training data for AI*

The already extensive use of systems with artificial intelligence requires the relevant data in order to create autonomous analyses and information. Insofar as the operator of the AI uses data from the other party, it must be clarified whether it is allowed to do so without receiving anything in return or whether the provider of the data should share in the results of the analyses.

## **Data protection and data security**

### *Data protection regulations*

Both parties are obliged to comply with the statutory provisions on the protection of personal data. This in particular applies if the supplier processes the customer's personal data. In this case, the supplier shall act as a commissioned data processor and shall be responsible for taking suitable measures to pseudonymise or anonymise the data in order to ensure the protection of privacy. The obligations may need to be agreed in a data processing agreement; in the case of data transfers abroad, it is necessary to check which requirements apply.

### *Protection of confidential information and trade secrets*

All data generated by the machine or through its maintenance should be classified as confidential information and considered trade secrets of the customer. Explicit labelling as confidential data should not be required to ensure its protection. The supplier may then only use this data to the agreed extent and

must ensure that it is protected against unauthorised access.

### *Safekeeping and security measures*

To ensure the protection of the data, both parties must take technical and organisational measures to protect the data provided from unauthorised access. This includes implementing suitable access rights, encryption systems and securing the data against physical and digital threats. The protection of personal data must be in accordance with the applicable data protection laws.

## **Warranty and liability**

### *Accuracy and completeness of the data*

The customer is responsible for the accuracy and completeness of the data provided. If the supplier receives or processes incorrect data, it is not liable for the resulting consequences or decisions. This regulation ensures clear responsibilities with regard to data processing.

### *Freedom from third-party rights:*

Each party must ensure that the data provided is free from third-party rights. This means that there are no exclusive rights or restrictions on the transmitted data that could restrict its use by the other party.

## **Data controls and reporting obligations**

Each party should have the right to monitor compliance with the protective provisions by means of checks. These can be carried out internally or by neutral third parties. In the event of unauthorised access to the data, the affected party must inform the other party immediately in order to minimise damage and take appropriate measures.



## Contract period and remuneration

The data transfer should take place during the entire term of the underlying contractual relationship. After termination of the contract, both parties are no longer obliged to exchange data, but may continue to store and use data already transmitted if this is necessary for future tasks.

In principle, data is provided free of charge, often as a prerequisite for the provision of other services, e.g. monitoring for *predictive maintenance*. However, if the scope of services is extended, both parties should agree on a possible fee. This applies in particular to the use of additional software or extended analyses that are not part of the original contract.

## Conclusion

This recommendation describes a comprehensive "Data Use Agreement" that serves as the basis for cooperation between supplier and customer. A clear regulation of rights, obligations and responsibilities when handling data ensures a transparent and legally secure basis that serves to protect trade secrets and optimise machine performance.

+ + +

## IMPRINT

### PUBLISHER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH  
Luisenstr. 5, D-30159 Hanover  
Phone 0511-307 56-0 Fax 0511-307 56-10  
Mail [info@herfurth.de](mailto:info@herfurth.de), Web [www.herfurth.de](http://www.herfurth.de)  
Hanover · Göttingen · Brussels  
Member of the ALLIURIS GROUP, Brussels

### EDITORIAL

Head: Ulrich Herfurth, lawyer, admitted in Hanover and Brussels (responsible)

Collaboration: Angelika Herfurth, Attorney-at-Law, FA Family Law; Sibyll Hollunder-Reese, M.B.L. (HSG), Attorney-at-Law; Günter Stuff; Xiaomei Zhang, Lawyer (China), Mag. iur. (D); Thomas Gabriel, Attorney-at-Law; JUDr. Yvona Rampáková, Lawyer (CR); Dr. Jona Aravind Dohrmann, Attorney-at-Law; Prof. Dr. jur. Jona Aravind Dohrmann, lawyer; Prof. Dr. Christiane Trüe LL.M. (East Anglia); Konstantin Kuhle, lawyer; Antonia Herfurth, lawyer, LL.M. (Göttingen); Sara Nesler, Mag. iur. (Torino), LL.M. (Münster).

### CORRESPONDENTS

Amsterdam, Athens, Brussels, Budapest, Helsinki, Istanbul, Copenhagen, Lisbon, London, Luxembourg, Milan, Madrid, Moscow, Paris, Stockholm, Warsaw, Vienna, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Beijing, Tokyo, among others.

### PUBLISHER

CASTON GmbH, Law & Business Information  
Luisenstr. 5, D-30159 Hanover,  
Phone 0511-307 56-50 Fax 0511-307 56-60  
Mail [info@caston.info](mailto:info@caston.info); Web [www.caston.info](http://www.caston.info)

All information is provided to the best of our knowledge; liability is limited to intent and gross negligence. Reproduction, even in part, only with the authorisation of the publisher.