

As approved by CEO on June, 2018.

LOGSTOR

Privacy Policy

1. Purpose and Scope

It is one of the fundamental principles of LOGSTOR International Sp. Z o.o. and its subsidiaries (together “LOGSTOR” or “the Company”) to strictly observe all national and international laws and regulations under which LOGSTOR is operating and to maintain high ethical standards in conducting its business.

It is the strong belief of LOGSTOR’s management that not only the interest of LOGSTOR, its employees and various stakeholders, but also the interest of society, is best served by a conduct in adherence with a policy which ensures protection of personal data. Therefore, it is the policy of LOGSTOR to strictly comply in all respects with the General Data Protection Regulation, including all national Data laws and regulations which strive to protect the individual’s personal data which in any way are controlled, owned or processed by LOGSTOR.

The General Data Protection Regulation is mandatory rules of law, which must be complied with at all times – also prior to the adoption of the first LOGSTOR Personal Data Protection Policy.

This Personal Data Protection Policy (“Policy”) comes into effect as per the date stated on the first page and is binding on all board members, directors, officers and employees of LOGSTOR. This Policy replaces any previous policy of personal data in effect at LOGSTOR.

2. Personal Data Protection Policy

2.1 Data Protection Officer - Contact Information

LOGSTOR is both considered Data Controller and Data Processor, and in that regard responsible for ensuring that personal data is processed in accordance with the applicable laws and regulations. LOGSTOR has internally appointed a Data Protection Officer (DPO), who is globally responsible for ensuring and supporting locally that rules and procedures regarding processing of personal data are observed in the daily business.

Any questions in relation to the processing of personal data within the Company, can be directed at the Data Protection Officer. Contact information of the Data Protection Officer is available [here](#).

2.2 Processing of personal data

LOGSTOR is solely processing personal data in a business-to-business setup, and does not in any way process consumer data.

LOGSTOR process two categories of data subjects, (1) any and all business partners, customers, suppliers and the like for which this Policy is applicable, (2) employees for which an internal policy is applicable.

2.3 Types of personal data

As described above this Policy concerns the processing of personal data of data subject category (1).

In this regard LOGSTOR will process personal data, which include amongst other:

Name - contact information - email address - telephone numbers - company where employed - job title – relevant social activity preferences - birthday - certification of skills – video surveillance

2.4 Purpose of processing personal data

LOGSTOR collect, store, process and delete personal data for legitimate business purposes in general. For example, when we need to:

Register in CRM or other similar systems - register in LOGSTOR Academy - distribute customer / business partner / supplier a courtesy gift in countries where relevant - keep record of certification of skills - send newsletters - have correspondence in relation to projects - distribute technical information / updates - in order to identify and comply with our obligations - in order to determine to sue or defend LOGSTOR against legal requirements - handle claims

2.5 The extent of data

LOGSTOR ensures that only personal data necessary for particular purposes are processed. Therefore, only the amount of data needed for each specific purpose is collected. It is ensured that the amount of processed data is not unnecessarily large, the storage time is not too long and only the relevant and necessary employees has access hereto.

LOGSTOR will before the processing of personal data, investigate whether it is possible to minimise the amount of personal data. LOGSTOR also investigate whether some of the data types we use may be used in anonymous or pseudonymised form. This will be done for all processing, unless LOGSTOR's obligations to public authorities or to daily business operations does not allow it.

LOGSTOR will only collect, process and store the personal data needed to meet the intended purpose. In addition, it may be decided by law what type of data it is necessary to collect and store for our business operations. The type and extent of the personal data LOGSTOR process may also be required to fulfill a contract or other legal obligation.

2.6 Control

LOGSTOR verify that the personal data we control, own or process are to the best of our knowledge not incorrect or misleading. LOGSTOR also make sure to update the personal data continuously.

LOGSTOR's administration of personal data is dependent on the personal data being correct and up to date, why it is important that business contacts, customers, suppliers or the like notifies when personal data in these relations should be edited, updated or deleted.

3. Rights of the registered

Anyone whose personal data LOGSTOR process (the "Registered") have a right of access to the personal data.

Furthermore, the Registered have the right to object to the collection and further processing of personal data. Moreover, the Registered have the right to rectification of personal data, or to require LOGSTOR to restrict the processing of the personal data.

If requested, LOGSTOR will delete the personal data which we store and process without undue delay, unless we may continue the processing on another legal basis, e.g. if the processing is necessary to defend a legal claim or to comply with a request from the registered.

Under certain circumstances, the Registered may also request that LOGSTOR provide an overview of the personal data in a structured, commonly used and machine-readable format and request to transmit such data to another data controller.

If the Registered wishes to exercise the rights as described above, please contact the DPO [here](#).

If the Registered disagree with how LOGSTOR process personal data or the purposes for which we process personal data, the Registered may either contact us, take legal actions at the ordinary courts or lodge a complaint with the local Data Authorities. A full list of national Data Authorities can be found [here](#).

4. Security

To protect the access to personal data by unauthorised persons, LOGSTOR uses IT solutions that automatically ensure that data is only available to relevant employees. There is also embedded protection against unlimited access to data.

LOGSTOR have also adopted internal rules on information security in our IT Policy that contain instructions and measures which protect your data against being destroyed, lost or modified, from unauthorised disclosure, and against unauthorised access or knowledge hereof.

5. Transfer

5.1 Transfer to third parties

As part of LOGSTOR's business, we are required to disclose personal data to third parties.

Third parties include amongst other:

- IT suppliers
- Sub-suppliers
- Customers
- Project managers
- Insurance company
- Insurance broker
- Transportation Companies
- Couriers

The disclosure of personal data must be substantively justified and, moreover, necessary for the provision of a legitimate interest of the employee, business partner, customer, supplier or the Company. Processing of personal data incompatible with the purposes which is the basis of the Company's processing must not occur.

Regardless of whether LOGSTOR transfer personal data to partners' resident in countries inside or outside the EU or EEA, we must always ensure that our level of privacy protection will comply with the requirements we have set in this policy and under applicable laws and regulations. Amongst other we ask for data processing agreements, information security and documentation of fulfillment of rights.

LOGSTOR is aware of the requirements for the content of data processing agreements and we always ensure that the necessary agreements are in place to secure personal data rights.

5.2 Transfer intercompany

As part of LOGSTOR's business, the disclosure of personal data between the LOGSTOR affiliates is a necessity for running the daily business.

In order to ensure to highest level of security possible, intercompany data processing agreements are made between all LOGSTOR affiliates. Each legal entity being both data controller and data processor means that the agreements are mutual in the obligations of both roles, ensuring that the General Data Protection Regulation and all national data laws and regulations are complied with.

6. Retention

LOGSTOR is required to retain certain records of personal data, for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

- Fines and penalties
- Loss of rights
- Obstruction of justice charges
- Contempt of court charges
- Serious disadvantages in litigation

We must retain certain records because they contain information that:

- Serves as LOGSTOR's corporate memory.
- Have enduring business value (for example, they provide a record of a business transaction, evidence LOGSTOR's rights or obligations, protect our legal interests or ensure operational continuity).
- Must be kept in order to satisfy legal, accounting or other regulatory requirements.

We must balance these requirements with our statutory obligation to only keep records for the period required and to comply with data minimisation principles of only keeping data as long as necessary.

7. Storage and deletion records of personal data

7.1 Storage

LOGSTOR's records of personal data must be stored in a safe, secure and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once a day and maintained off site.

7.2 Deletion

LOGSTOR is responsible for the continuing process of identifying the records that have met their required retention period and supervising their deletion. The deletion of personal data, confidential, financial and personnel-related records must be conducted by shredding. The deletion of electronic records must be coordinated with the IT Department / Manager.

8. Implementation and Compliance

Where a LOGSTOR company is a participant in any joint venture or commercial sharing arrangement, LOGSTOR seeks, as far as practicable, to ensure that the combined vehicle complies with our Policies.

In order to ensure that all relevant Employees are trained in the content of this Policy, hereunder measures to ensure compliance with this Policy, LOGSTOR have implemented various training initiatives, including an e-learning program. LOGSTOR will continuously strive to optimise its efforts in this regard.

If you become aware of any suspected or actual breaches of our Policy, please inform the Data Protection Officer or Legal Department. All reports are treated confidentially and investigated properly and promptly.

In case of any questions about this Policy, or the applicable legislation you should contact the Data Protection Officer.

The Policy can be provided in hard copy upon request to the Data Protection Officer. Disregard or breach of the Group Policy by an employee may result in disciplinary action.

9. Amendments

We reserve the right to amend this privacy policy based on substantial changes in the legislation, new technical solutions, new or improved functions and to improve the website.