DS/
better together

PRIVACY *policy*

for the Protection of Personal Data
of the Diersch & Schröder Group
Status 2023

ENERGY

DS / WESER-PETROL

DS / MINERALÖL

DS / CARD+DRIVE

/ CARD+DRIVE Polska

LANFER ENERGIE

EMOVA
Energie. So einfach.

UTG
Unabhängige Tanklogistik GmbH

ENERGU

HAUER

WESER TANKING

LEU.

CHEMICALS

ADDITIV CHEMIE LUERS

ESTICHEM AS

ACF

LEVACO CHEMICALS

Sparks

YOUNG BUSINESS

SCS

ELAPRO

ecopox

polytives

Lynatox


DS
DIERSCH &
SCHRÖDER

CONTENTS

FOREWORD

Dear Readers,

We, Diersch & Schröder GmbH & Co. KG and our affiliated companies (hereinafter: "DS Group"), are aware of the great significance of protecting personal data. This applies to personal data of our customers, business partners, shareholders and especially of our employees.

Safeguarding data protection is the basis for trusting business relationships and for the reputation of the DS Group as an attractive employer.

In this Privacy Policy, we have set out the **requirements for the processing of personal data**. This Policy complies with the requirements of the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and the European General Data Protection Regulation (GDPR) and ensures compliance with the principles of data protection law.

It defines the applicable data protection standard within the DS Group.

Bremen, December 1, 2023

Jan Christiansen

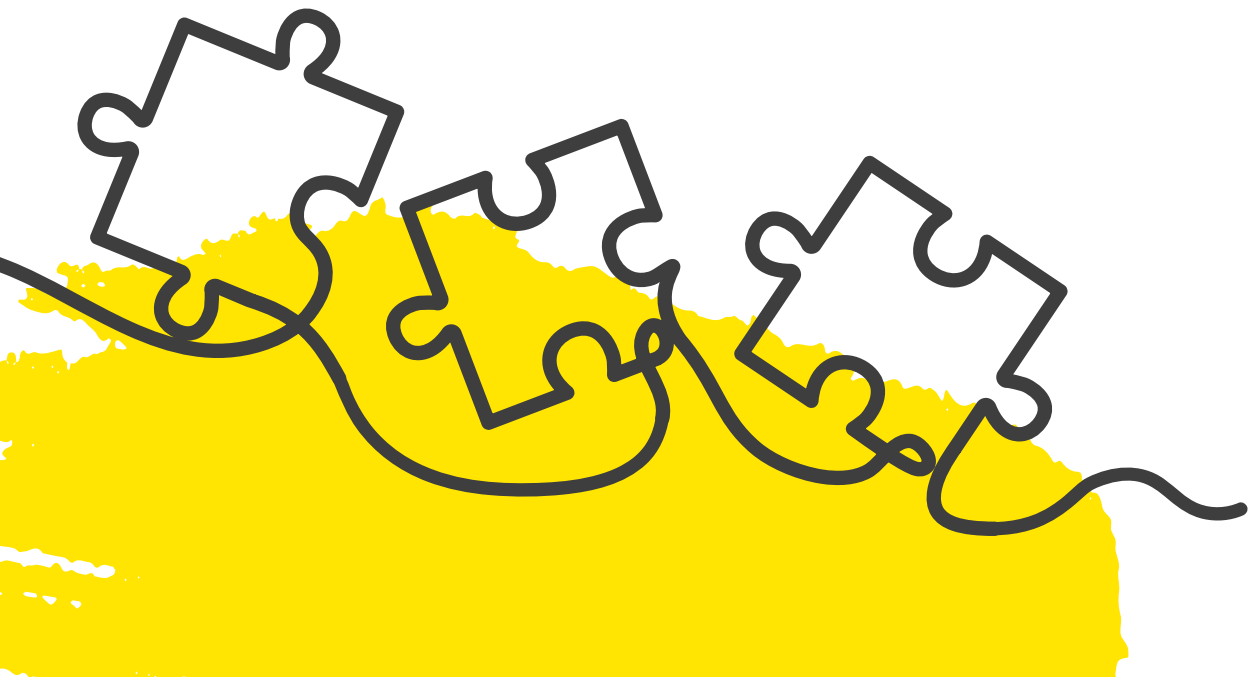
Jan Christiansen
Chief Executive Officer
of the Diersch & Schröder Group

1 Objective of the Privacy Policy

1. This Policy serves as the binding basis for the legally compliant handling of personal data within the DS Group.
2. It shall define the fundamental rights of Data Subjects, in particular their right to the protection of personal data.
3. The current version of this Policy is available to all employees at all times www.ds-bremen.com/en/responsibility.

2 Scope

1. This Policy applies to the DS Group. For DS Group companies with registered office or a branch outside the European Union, this Policy is supplemented by additional policies for the protection of personal data if this is required under the respective applicable national Law.
2. The requirements and prohibitions of this Policy apply to all processing of personal data.
3. It applies personally to all employees of the DS Group and as an amendment to any regulation in their employment contracts.



3 Responsibility and Data Protection Officer

1. The Managing Director (phG) of Diersch & Schröder GmbH & Co KG and the Compliance Officer of the DS Group are responsible for the content of this Privacy Policy.
2. The respective Managing Director(s) of the subsidiaries of the DS Group are responsible for compliance with and implementation of the Privacy Policy. The Data Protection Officer, the Compliance Officer of the DS Group and the employee responsible for data protection (if this position exists in the respective company) shall support them.
3. A Data Protection Officer must be appointed for each subsidiary of DS Group if:
   - ten people at the company are continually engaged in the automated processing of personal data, or
   - the company employs more than twenty employees.

   The position of Data Protection Officer may be filled internally or externally. Each company of DS Group has the option to appoint the Data Protection Officer that is already appointed for a part of the DS Group.
4. The Data Protection Officer is available to advise the Managing Director(s) on the performance of their obligations under data protection law, monitors conformity with statutory requirements and any risks, and is responsible for consultations with the supervisory authorities. In all other respects, the Data Protection Officer works free of instructions, conscientiously and in accordance with their expertise.
5. The Data Protection Officer may be contacted at any time in confidence with complaints, requests for information and other data protection concerns. The Data Protection Officer can be contacted at: **datenschutz@ds-bremen.de**.

4 Definitions

In accordance to Art. 4 of the European General Data Protection Regulation (GDPR), this Privacy Policy is based on the definitions set out in Annex 1.

5 Our priciples for the processing of personal data

The following statutory principles must be observed when processing personal data (cf. Article 5 GDPR):

1. Lawfulness: Personal data are collected in accordance to the Law.

2. Purpose limitation: Personal data must be used for specified and legitimate purposes and not in a manner that is incompatible with those purposes.

3. Transparency: Personal data are to be handled in a manner that is transparent and comprehensible. The Data Subject must be notified accordingly as defined in Article 13 GDPR. The information should clarify the purpose of the data processing, the contact details of a responsible body and whether or to which third parties the data will be transmitted.

4. Data economy; storage limitation: Before processing personal data, it must always be checked if and to what extent the processing purpose is achieved with the intended procedure. If the purpose can also be achieved without recourse to personal data, for example through anonymized or pseudonymized data, this milder approach is preferable. Data should only be stored for as long as it is necessary for the processing purpose.

5. Accuracy; timeliness of data: The accuracy, completeness and timeliness of the personal data collected must be ensured. Otherwise, incorrect, incomplete and data that are no longer up to date must be rectified, supplemented, updated or erased without delay.

6. Integrity; confidentiality: Personal data must be treated confidentially and appropriate technical as well as organizational measures must be taken to ensure adequate protection against unauthorized or unlawful processing and against accidental loss or damage.

7. Erasure: As soon as the statutory or operational retention periods have expired, personal data must be erased.

8. Documentation; record of processing activities: The respective DS company must maintain a written or electronic record of all data processing activities that complies with the minimum information requirements set out in Article 30 (1) and (2) GDPR. DS Group uses the PRIVACY PORT tool for this purpose. The Data Protection Officer and the Compliance Officer are available to the Controller in an advisory capacity.

6 Lawfulness of data processing

According to Section 26 BSDG, Article 6 (1) GDPR, the processing of personal data is lawful only if one of the following applies:

Consent to data processing: The Data Subject may give their consent to the processing for specific purposes, in particular for advertising purposes. The declaration of consent must be made voluntarily and generally in writing or electronically. Consent must be properly documented. As soon as the Data Subject objects to the use of the data for advertising purposes, their personal data must be made unavailable and the data must not be used again.

Data processing based on contractual relations and legal obligation: Processing is permitted if it is necessary for the performance of an existing contract or a pre-contractual measure or a legal obligation of the Controller.

Data processing based on legitimate interests: Processing is permitted if it is necessary in order to protect the vital interests of the Data Subject or another natural person. In addition, processing may be carried out to protect the legitimate interests of the Controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require the protection of personal data. This must be carefully checked prior to any processing.

Statutory permission to process data: Processing is permitted if it is required or permitted by national law.

Data processing of especially sensitive data: Especially sensitive personal data may be processed only if the Data Subject's consent has been obtained or if it is permitted by law or necessary for the defense of legal claims against the Data Subject.

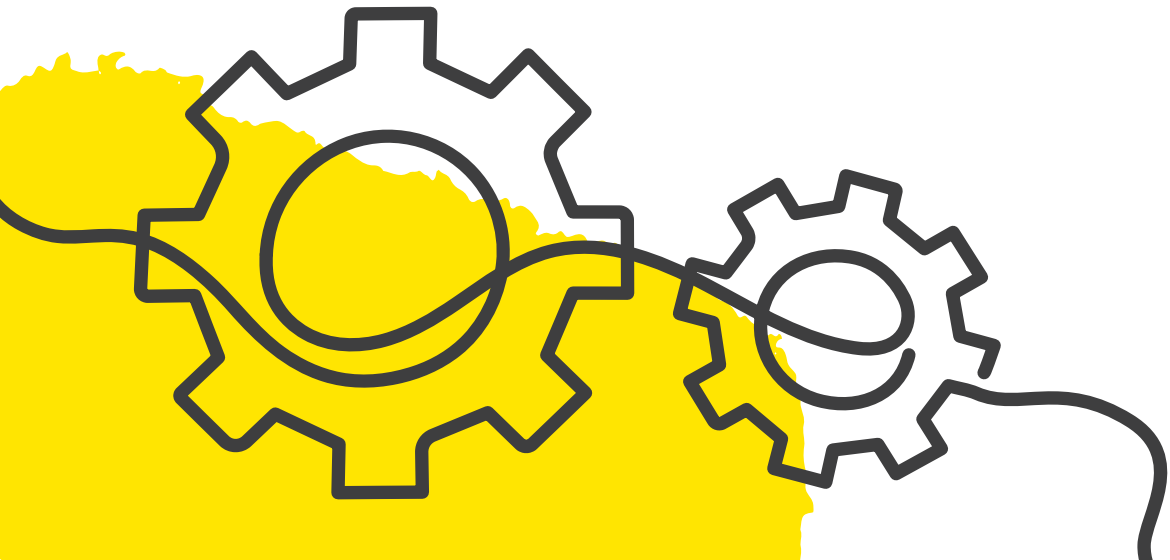
Personal data on the Internet and tracking: If personal data are processed, collected or used on websites or in apps or by means of cookies, there is always an obligation to inform the Data Subject about this in an easily recognizable manner by means of notices. The same applies to tracking, the creation of usage profiles to evaluate online usage behavior. Personal tracking is permitted only where allowed by law or with the Data Subject's consent.

7 Lawfulness of the data transfer

1. The transfer of personal data to third parties is permitted only under the conditions of this Privacy Policy for lawful data processing. Consequently, a transfer is allowed if the Data Subject has given its consent, a joint data processing agreement or an agreement in accordance to Article 26 GDPR has been signed, or if it is permitted by law and serves a specified purpose.
2. In the event of a data transfer to a recipient outside the European Economic Area, an adequate level of data protection must be ensured that is equivalent to that of this Privacy Policy (see also Articles 44 et seqq. GDPR

8 Data processing and data protection agreements

1. If an external natural or legal person, authority or other institution processes personal data on behalf of the Controller, a data processing agreement must be concluded with the contractor in writing with the content required by Article 28 GDPR.
2. This also applies to the joint processing of data by affiliated companies of DS Group. At best, this processing should be regulated by (a) group-wide agreement(s) in accordance with Article 26 GDPR (so-called “Master (Data) Agreement”).
3. The company of DS Group managing the process (in case of Article 26, Article 28 GDPR) bears the responsibility for the compliant execution and implementation of the processing.



9 Data protection impact assessment

1. If a form of processing of personal data is likely to present a high risk to the rights and of the Data Subject, there is an obligation to carry out a data protection impact assessment of the intended data processing in advance. The data protection impact assessment is to comply with the minimum requirements set out in Article 35 (7) GDPR.
2. For the performance of the data protection impact assessment, the Data Protection Officer provides advice and support.

10 Rights of data subjects

In accordance with the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG), Data Subjects may exercise the following data protection rights, provided that the requirements of the respective standards are met. To exercise a data protection right, the Data Subject may contact the company's internal Data Protection Officer. The Data Subject must be notified within one month of the implemented measure.

10.1 Right of Access, Article 15 GDPR, Section 34 BDSG

The Data Subject has the right to obtain information as to whether or not personal data concerning them are being processed in the company and, where that is the case, about the categories of processed data, the purpose of processing and the period for which the data will be stored.

10.2 Right of Recitification, Article 16 GDPR

The Data Subject may obtain the rectification or completion of personal data concerning them that are inaccurate or incomplete.

10.3 Right to Erasure ("Right to be Forgotten"), Article 17 GDPR, Section 35 BDSG

The Data Subject has the right to obtain the erasure of personal data if the following applies:

- The purpose of data processing does not or no longer exist.
- There is no legal ground for the data processing or it has ceased to exist as the Data Subject has withdrawn their consent.
- The Data Subject objects to the data processing and there are no overriding legitimate grounds for the processing.
- The data have been unlawfully processed.
- The processing of personal data is not (or no longer) necessary for compliance with a legal obligation or for the defense of legal claims.
- There is no public interest in the processing overriding the rights of the Data Subject.

10.4 Right of Restriction of Processing, Article 18 GDPR

1. The Data Subject has the right to restrict the processing of personal data if one of the following applies:
    - The accuracy of the personal data is contested by the Data Subject. A restriction is made for the period enabling the Controller to verify the accuracy.
    - The data processing is unlawful, but the Data Subject requests the restriction of use instead of erasure of the personal data.
    - The Controller no longer needs the personal data for the purposes of processing, but the Data Subject needs them for the defense of legal claims.
    - The Data Subject has objected to the processing. Processing is restricted pending the Controller's verification of the objection.
2. Where processing has been effectively restricted, the personal data concerned may only be processed with the Data Subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of others or for reasons of important public interest.

10.5 Right of Data Portability, Article 20 GDPR

If the data processing is based on consent or was necessary for the performance of a contract, the Data Subject has the right to receive and transfer the personal data concerning them to another Controller, where this is technically feasible.

10.6 Right to Object, Article 21 GDPR

The Data Subject has the right to object at any time to data processing based on consent or necessary to protect legitimate interests. For this purpose, an assessment must show that the Data Subject's legitimate interest overrides the company's interest in processing. There is no right to object if the processing serves the defense of legal claims.

10.7 Right to Lodge a Complaint with a Supervisory Authority, Article 77 GDPR ICW Section 19 BDSG

In addition, the Data Subject has the right to issue a complaint with the competent supervisory authority if they consider that the processing of personal data relating to them has been carried out unlawfully.

11 Confidentiality of data processing

All employees of DS-Group are subject to the obligation to comply with data protection (“data secrecy”). Unauthorized collection, processing or use of personal data is prohibited.

1. All employees must agree to confidentiality in writing before commencing their work. The relevant templates are available from the HR Department of Diersch & Schröder GmbH & Co KG. Assurance must be given that the personal data obtained in the course of their activity will not be used for private or commercial interests, not forwarded to unauthorized persons and not made accessible in any other way. This obligation survives the end of the employment relationship.
2. To ensure a high level of confidentiality, employees may be granted access to personal data only where this is specifically necessary for the performance of their activities (“need-to-know principle”).

12 Data security and training

1. The protection of personal data against unauthorized access, unlawful processing or unauthorized loss, alteration or destruction must be ensured. Effective technical and organizational measures must be compiled in a security concept, reflecting the current state of the art, the risks specific to processing and the legitimacy of the processed data.
2. These measures must also be observed prior to any introduction of new IT systems for data processing.
3. The security concept is to be continuously reviewed and adapted to technical and organizational changes and developments in the protection of personal data.
4. In order to maintain a high level of data protection in the company, those employees who regularly or continuously process or have access to personal data must be trained to the necessary extent on data protection requirements.

13 Data protection and monitoring

1. To ensure an adequate level of protection and conformity with applicable data protection regulations, compliance with this policy is reviewed periodically. Such monitoring is the responsibility of the Compliance Officer of the DS Group, the Data Protection Officer or an auditor entrusted with audit rights. Audit results must be documented.
2. Data privacy monitoring has been successfully completed when all documented deficiencies have been remedied by implementing appropriate measures. This must be checked accordingly.

14 Data protection incidents and legal consequences of violations

1. In the event of a data protection incident, a breach of this Policy or of other regulations on the protection of personal data, the employee responsible is obligated to promptly report the data protection incident to their line manager as well as to the Data Protection Officer at **datenschutz@ds-bremen.de**. All information necessary for clarifying the facts must be provided, primarily about the recipient, the specific personal data concerned as well as type and scope of the data affected by the incident.
2. In case of a reporting obligation to the supervisory authorities for the respective data protection incident, the Data Protection Officer must promptly fulfill this obligation.
3. If a data protection incident, a breach of this Policy or a breach of other data protection regulations has been caused negligently or intentionally, this will entail consequences under employment law. In addition, criminal and civil sanctions may be considered, such as the assertion of claims for damages.

Important Information

This privacy policy cannot provide specific answers to all questions and situations. If further information is required, the Compliance Officer can be contacted at **compliance@ds-bremen.de** at any time.

Annex 1

Personal data (cf. Article 4 No. 1 GDPR) means any information relating to a natural person who can be identified or is identifiable, directly or indirectly, by such information. A person is identifiable as soon as a link can be established to them by means of personal data, in particular by reference to an identifier, location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. This is also the case if an inference to a natural person is possible through a combination of information - even if only linked with incidental additional knowledge. Personal data includes, in particular, the name, address, telephone number, private e-mail address, or photos and video recordings of the natural person, as well as customer and personal data. Identification of the person can be excluded with the help of anonymization or pseudonymization.

Especially sensitive personal data include any information revealing a Data Subject's racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, health or sexual orientation or sex life.

A **Data Subject** is any natural person about whom personal data are processed.

Processing of personal data (cf. Article 4 No. 2 GDPR) means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing (cf. Article 4 No. 3 GDPR) means the marking of stored personal data with the aim of limiting their processing in the future.

Transfer means any disclosure of personal data by the Controller to third parties.

Profiling (Article 4 No. 4 GDPR) means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Anonymization means the processing of personal data in such a manner that a reference to a person can no longer be established in the long term or that it is only possible to draw conclusions about a natural person with disproportionate effort.

Pseudonymization (Article 4 No. 5 GDPR) means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Filing system (Article 4 No. 6 GDPR) means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Controller (Article 4 No. 7 GDPR) means the natural or legal person, public authority, agency or other body which, alone or jointly with others determines, the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for under Union or Member State law.

Processor (Article 4 No. 8 GDPR) means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Recipient (Article 4 No. 9 GDPR) means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law are not regarded as recipients; the processing of those data by those public authorities is to be carried out in compliance with the applicable data protection rules according to the purposes of the processing.

Third party (Article 4 No. 10 GDPR) means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, processor and persons who, under the direct authority of the Controller or the processor, are authorized to process the personal data.

Consent (Article 4 No. 11 GDPR) of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies their agreement to the processing of personal data relating to them.

Personal data breach (Article 4 No. 12 GDPR) means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to. personal data transmitted, stored or otherwise processed.

Data concerning health (Article 4 No. 15 GDPR) means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.

Enterprise (Article 4 No. 18 GDPR) means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Group of undertakings (Article 4 No. 19 GDPR) means a controlling undertaking and its controlled undertakings.

Data protection incident refers to all circumstances giving rise to the suspicion that personal data have been unlawfully collected, transmitted, copied, used or spied out by employees or third parties.

DS/
better together

ENERGY

Better together for **mobility, heat and electricity** – that's what drives us.

CHEMICALS

Our **additives** lubricate industrial production equipment and protect banana plants.

YOUNG BUSINESS

Start-ups help the DS Group to stay **young** and **innovative**.