

# *DATEN* **SCHUTZ** **RICHTLINIE**

zum Schutz personenbezogener Daten  
der Diersch & Schröder Unternehmensgruppe  
Stand 2023

# ENERGIE

**DS** // WESER-PETROL

**DS** // MINERALÖL

**DS** // CARD+DRIVE

**CARD+DRIVE**  
Polska

**LANFER**  
ENERGIE

**E M O V A**  
Energie. So einfach.

**UTG**  
Unabhängige Tanklogistik GmbH

**ENERGU**

**HAUER**

**WESER**  
**TANKING**

**LEU.**

# CHEMIE

**ADDITIV**  
**CHEMIE**  
**LUERS**

**ESTICHEM**<sup>AS</sup>

**ACF**

**LEVACO**  
CHEMICALS

**Sparks**

# YOUNG BUSINESS

**SCS**

**ELAPRO**

**ecopox**

**polytives**

**Lynatox**



# INHALT

SEITE	KAPITEL
04	Vorwort
05	Bedeutung und Ziel der Datenschutzrichtlinie
05	Geltungsbereich
06	Verantwortlichkeit und Datenschutzbeauftragter
06	Begriffsbestimmungen
07	Unsere Grundsätze für die Verarbeitung von personenbezogenen Daten
08	Rechtmäßigkeit der Datenverarbeitung
09	Rechtmäßigkeit der Datenübermittlung
09	Auftragsdatenverarbeitung und datenschutzrechtliche Vereinbarungen
10	Datenschutz-Folgenabschätzung
10	Recht der Betroffenen
14	Vertraulichkeit der Datenverarbeitung
13	Datensicherheit und Fortbildungen
14	Datenschutzkontrolle
14	Datenschutzvorfälle und Rechtsfolgen von Verstößen
16	Anlage 1

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

wir, die Diersch & Schröder GmbH & Co. KG und ihre verbundenen Unternehmen (nachfolgend „DS-Gruppe“), sind uns der **hohen Bedeutung des Schutzes personenbezogener Daten** bewusst. Dies gilt für personenbezogene Daten unserer Kundinnen und Kunden, Geschäftspartnerinnen und Geschäftspartnern, Gesellschafterinnen und Gesellschaftern und insbesondere unserer Mitarbeiterinnen und Mitarbeiter.

Die Wahrung des Datenschutzes ist Grundlage für vertrauensvolle Geschäftsbeziehungen und die Reputation der DS-Gruppe als attraktiver Arbeitgeber.

In dieser Richtlinie zum Datenschutz haben wir die **Anforderungen an die Verarbeitung personenbezogener Daten** festgelegt. Diese Richtlinie entspricht den Anforderungen des Bundesdatenschutzgesetzes (BDSG) sowie der europäischen Datenschutz-Grundverordnung (DSGVO) und stellt die Einhaltung der Grundsätze des Datenschutzrechts sicher.

Sie legt den gültigen Datenschutzstandard innerhalb der DS-Gruppe fest.

Bremen, den 01.12.2023

Jan Christiansen



**Jan Christiansen**

Chief Executive Officer  
der DS-Unternehmensgruppe



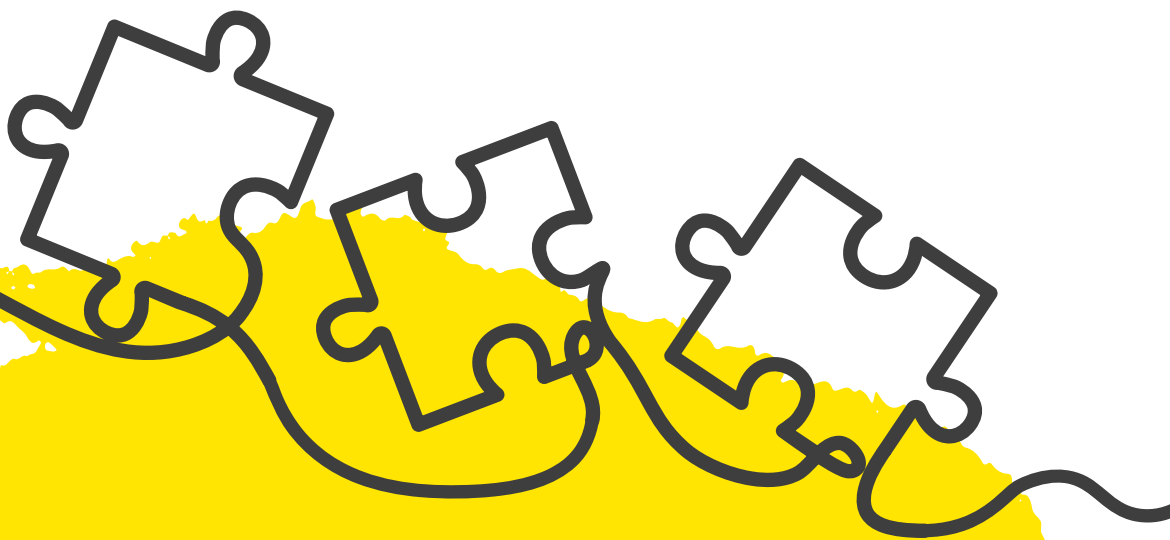


## **1 Bedeutung und Ziel der Datenschutzrichtlinie**

1. Diese Richtlinie ist die verbindliche Basis für den rechtskonformen Umgang von personenbezogenen Daten in der DS-Gruppe.
2. Mit dieser Richtlinie sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, gewahrt und geschützt werden.
3. Die aktuelle Version dieser Richtlinie ist für alle Mitarbeiterinnen und Mitarbeiter jederzeit zugänglich unter [www.ds-bremen.com/verantwortung](http://www.ds-bremen.com/verantwortung).

## **2 Geltungsbereich**

1. Diese Richtlinie findet Geltung für die DS-Gruppe. Für Unternehmen der DS-Gruppe, die ihren Sitz oder eine Niederlassung außerhalb der Europäischen Union haben, wird diese Richtlinie durch weitere Richtlinien zum Schutz von personenbezogenen Daten ergänzt, wenn dies nach dem jeweils geltenden nationalen Recht erforderlich ist.
2. Die Gebote und Verbote dieser Richtlinie gelten für sämtliche Verarbeitungen personenbezogener Daten.
3. Sie gilt persönlich für alle Mitarbeiterinnen und Mitarbeiter der DS-Gruppe und in Ergänzung zu etwaigen arbeitsvertraglichen Regelungen.



## 3 Verantwortlichkeit und Datenschutzbeauftragter

1. Die Geschäftsführung (phG) der Diersch & Schröder GmbH & Co. KG und der Compliance Officer der DS-Gruppe sind für den Inhalt dieser Datenschutzrichtlinie verantwortlich.
2. Die jeweilige Geschäftsführung des Unternehmens der DS-Gruppe ist verantwortlich für die Einhaltung und Umsetzung der Datenschutzrichtlinie. Der Datenschutzbeauftragte, der Compliance Officer der DS-Gruppe und der zuständige Mitarbeiter/ die zuständige Mitarbeiterin für Datenschutz (soweit in dem jeweiligen Unternehmen vorhanden) sollen sie hierbei unterstützen.
3. Für jedes Unternehmen der DS-Gruppe ist ein Datenschutzbeauftragter zu bestellen, wenn
  - in dem Unternehmen zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder
  - das Unternehmen mehr als zwanzig Mitarbeiterinnen und Mitarbeiter beschäftigt.

Die Position des Datenschutzbeauftragten kann unternehmensintern und extern besetzt werden. Für jedes Unternehmen besteht die Möglichkeit, die bereits benannten (Teil-) Konzern-Datenschutzbeauftragten ebenfalls zu beauftragen.

4. Der Datenschutzbeauftragte steht der Geschäftsführung bei der Erfüllung ihrer datenschutzrechtlichen Verpflichtungen beratend zur Verfügung, überwacht die Konformität mit gesetzlichen Vorgaben und etwaige Risiken und ist für Rücksprachen mit den Aufsichtsbehörden zuständig. Im Übrigen arbeitet er/sie weisungsfrei, gewissenhaft und entsprechend seines/ihrer Fachwissens.
5. An den Datenschutzbeauftragten kann sich jederzeit vertrauensvoll mit Beschwerden, Auskunftersuchen und sonstigen datenschutzrechtlichen Anliegen gewendet werden. Eine Kontaktaufnahme kann über **[datenschutz@ds-bremen.de](mailto:datenschutz@ds-bremen.de)** erfolgen.

## 4 Begriffsbestimmungen

Nach dem Vorbild des Art. 4 der europäischen Datenschutzgrundverordnung (DSGVO) liegen dieser Datenschutzrichtlinie die in Anlage 1 genannten Begriffsbestimmungen zu Grunde.



## Unsere Grundsätze für die Verarbeitung von personenbezogenen Daten

Bei der Verarbeitung personenbezogener Daten müssen die folgenden gesetzlichen Grundsätze eingehalten werden (vgl. Art. 5 DSGVO):

- 1. Rechtmäßigkeit:** Personenbezogene Daten werden auf rechtmäßige Weise erhoben.
- 2. Zweckbindung:** Die Nutzung personenbezogener Daten muss einem vorher festgelegten und legitimen Zweck dienen und darf nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise erfolgen.
- 3. Transparenz:** Der Umgang mit personenbezogenen Daten soll auf eine für die Betroffene/den Betroffenen nachvollziehbare, transparente Weise erfolgen. Er/Sie ist darüber i.S.d. Art. 13 DSGVO zu informieren. Aus der Information soll für die Betroffene/den Betroffenen ersichtlich sein, welchem Zweck die Datenverarbeitung dient, an welche verantwortliche Stelle er/sie sich wenden kann und ob bzw. an welche Dritte die Daten übermittelt werden.
- 4. Datensparsamkeit; Speicherbegrenzung:** Es ist stets vor der Verarbeitung personenbezogener Daten zu prüfen, ob und inwiefern der Zweck der Verarbeitung mit der beabsichtigten Vorgehensweise erreicht wird. Sofern der Zweck auch ohne Rückgriff auf personenbezogene Daten erreicht werden kann, etwa durch anonymisierte oder pseudonymisierte Daten, ist diese mildere Vorgehensweise vorzuziehen. Die Speicherung von Daten soll nur so lange erfolgen, wie sie für den Verarbeitungszweck erforderlich ist.
- 5. Richtigkeit; Datenaktualität:** Die Richtigkeit, Vollständigkeit und Aktualität der erhobenen personenbezogenen Daten sind sicherzustellen. Anderenfalls sind unrichtige, unvollständige und nicht mehr aktuelle Daten unverzüglich zu berichtigen, zu ergänzen, zu aktualisieren oder zu löschen.
- 6. Integrität; Vertraulichkeit:** Personenbezogene Daten sind vertraulich zu behandeln und durch geeignete technische wie auch organisatorische Maßnahmen sicherzustellen, dass ein angemessener Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust oder unbeabsichtigter Schädigung gewährleistet wird.
- 7. Löschung:** Sobald die gesetzlichen oder betriebsbedingten Aufbewahrungsfristen abgelaufen sind, sind personenbezogene Daten zu löschen.
- 8. Dokumentation; Verarbeitungsverzeichnis:** Über alle Datenverarbeitungen hat das Unternehmen schriftlich oder elektronisch ein Verzeichnis zu führen, das den in Art. 30 Abs. 1, Abs. 2 DSGVO vorgeschriebenen Mindestangaben entspricht. Die DS-Gruppe nutzt hierfür das Tool PRIVACY PORT. Dem Verantwortlichen steht der Datenschutzbeauftragte und der Compliance Officer beratend zur Seite.



## **Rechtmäßigkeit der Datenverarbeitung**

Nach §26 BDSG, Art. 6 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn einer der folgenden Erlaubnistatbestände vorliegt:

**Einwilligung in die Datenverarbeitung:** Die Betroffene/der Betroffene kann ihre/seine Einwilligung zur zweckbezogenen Verarbeitung, insbesondere zur werblichen Ansprache, geben. Die Einwilligungserklärung muss freiwillig und grundsätzlich schriftlich oder elektronisch erfolgen. Die Einwilligung muss ordnungsgemäß dokumentiert werden. Sobald der Verwendung der Daten zu Werbezwecken durch die Betroffene/den Betroffenen widersprochen wird, muss eine Sperrung seiner personenbezogenen Daten erfolgen und eine erneute Verwendung dieser Daten unterlassen werden.

**Datenverarbeitung aufgrund vertraglicher Beziehungen und gesetzlicher Verpflichtung:** Die Verarbeitung ist zulässig, soweit sie für die Erfüllung eines bestehenden Vertrages oder einer vorvertraglichen Maßnahme oder einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist.

**Datenverarbeitung aufgrund lebenswichtiger und berechtigter Interessen:** Die Verarbeitung ist zulässig, soweit sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist. Zudem darf eine Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dies ist vor jeder Verarbeitung sorgfältig zu prüfen.

**Gesetzliche Erlaubnis zur Datenverarbeitung:** Die Verarbeitung ist zulässig, wenn sie durch nationale Rechtsvorschriften verlangt, vorausgesetzt, gestattet oder auf andere Weise erlaubt wird.

**Datenverarbeitung bei besonders schutzwürdigen Daten:** Besonders schutzwürdige personenbezogene Daten dürfen nur dann verarbeitet werden, wenn eine Einwilligung der betroffenen Person vorliegt oder sie gesetzlich erlaubt oder zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche gegen den Betroffenen erforderlich ist.

**Personenbezogene Daten im Internet und Tracking:** Werden personenbezogene Daten auf Internetseiten oder in Apps oder mittels Cookies verarbeitet, erhoben oder genutzt, besteht in jedem Fall die Pflicht, die betroffene Person in leicht erkennbarer Weise darüber durch Hinweise zu informieren. Gleiches gilt für das Tracking, dem Erstellen von Nutzungsprofilen zur Auswertung des Internetnutzungsverhalten. Personenbezogenes Tracking ist ausschließlich aufgrund eines gesetzlichen Erlaubnistatbestandes oder der Einwilligung der Betroffenen/des Betroffenen zulässig.



## Rechtmäßigkeit der Datenübermittlung

1. Eine Übermittlung personenbezogener Daten an Dritte ist nur unter den Voraussetzungen dieser Datenschutzrichtlinie für eine rechtmäßige Datenverarbeitung zulässig. Folglich ist eine Übermittlung nur dann rechtmäßig, wenn eine Einwilligung der betroffenen Person vorliegt, eine Auftragsdatenverarbeitungsvereinbarung oder ein Vertrag zur gemeinsamen Verantwortung nach Art. 26 DSGVO gezeichnet wurde oder sie gesetzlich erlaubt ist und sie einem vorher festgelegten Zweck dient.
2. Bei einer Datenübermittlung an einen Empfänger außerhalb der Europäischen Wirtschaftsraumes muss ein angemessenes Datenschutzniveau sichergestellt werden, dass dem dieser Datenschutzrichtlinie (siehe auch Art. 44ff DSGVO) gleichwertig ist.



## Auftragsdatenverarbeitung und datenschutzrechtliche Vereinbarungen

1. Verarbeitet eine externe natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag des Verantwortlichen ist mit dem Auftragnehmer schriftlich eine Auftragsdatenverarbeitungsvereinbarung mit dem in Art. 28 DSGVO zwingend vorausgesetztem Inhalt zu schließen.
2. Dies gilt ebenfalls für die gemeinsame Verarbeitung von Daten durch verbundene Unternehmen der DS-Gruppe. Diese Verarbeitung soll bestenfalls durch (eine) konzernübergreifende Vereinbarungen(n) nach Art. 26 DSGVO geregelt werden (sog. „Master (Data) Agreement“).
3. Das beauftragende bzw. prozessführende (bei Art. 26, Art. 28 DSGVO Unternehmen trägt die Verantwortung für die rechtskonforme Durchführung und Umsetzung der Verarbeitung.

## 9 Datenschutz-Folgenabschätzung

1. Weist eine Form der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen auf, besteht im Vorfeld die Pflicht, eine Folgenabschätzung der angestrebten Datenverarbeitung für den Datenschutz durchzuführen. Die Datenschutz-Folgenabschätzung soll den in Art. 35 Abs. 7 DSGVO genannten Mindestvoraussetzungen entsprechen.
2. Für die Durchführung der Datenschutz-Folgenabschätzung steht der Datenschutzbeauftragte unterstützend zur Seite.

## 10 Rechte der Betroffenen

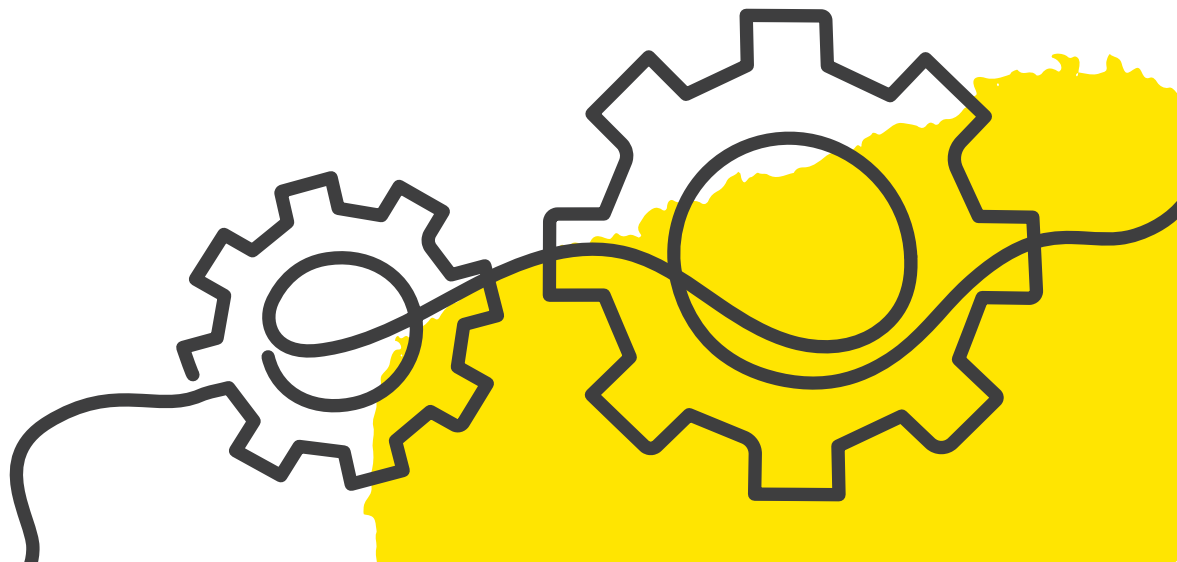
Gemäß der Europäischen Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) können die Betroffenen folgende Datenschutzrechte ausüben, sofern die Tatbestandsvoraussetzungen der jeweiligen Normen erfüllt sind. Um ein Datenschutzrecht auszuüben, kann sich der Betroffene an den unternehmensinternen Datenschutzbeauftragten wenden. Der betroffenen Person ist innerhalb eines Monats die durchgeführte Maßnahme anzuzeigen.

### 10.1 Recht auf Auskunft, Art. 15 DSGVO, § 34 BDSG

Der Betroffene/die Betroffene hat das Recht Auskunft darüber zu verlangen, ob im Unternehmen ihn/sie betreffende personenbezogene Daten verarbeitet werden, und bejahendenfalls welche Daten zu welchem Zweck und aus welcher Herkunft und in welcher Dauer gespeichert sind.

### 10.2 Recht auf Berichtigung, Art. 16 DSGVO

Der Betroffene/die Betroffene kann die Berichtigung oder Ergänzung der ihn betreffenden personenbezogenen Daten verlangen, die unrichtig oder unvollständig sind.



### **10.3 Recht auf Löschung („Recht auf Vergessenwerden“), Art. 17 DSGVO, § 35 BDSG**

Der Betroffene/die Betroffene hat einen Anspruch auf Löschung der ihn betreffenden personenbezogenen Daten, sobald einer der folgenden Lösungsgründe einschlägig ist:

- Der Zweck der Datenverarbeitung besteht nicht oder nicht mehr.
- Eine Rechtsgrundlage für die Datenverarbeitung fehlt oder ist weggefallen, indem der Betroffene seine Einwilligung widerrufen hat.
- Der Betroffene widerspricht der Datenverarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die Datenverarbeitung ist unrechtmäßig.
- Zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ist die Verarbeitung personenbezogener Daten nicht (mehr) erforderlich.
- Ein die Rechte des Betroffenen überwiegendes öffentliches Interesse an der Verarbeitung besteht nicht.

### **10.4 Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO**

1. Die betroffene Person hat das Recht auf Einschränkung der Verarbeitung der sie betreffenden personenbezogenen Daten, sobald einer der folgenden Gründe einschlägig ist:
  - Die Betroffene/der Betroffene bestreitet die Richtigkeit der personenbezogenen Daten. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche die Richtigkeit überprüft
  - Die Datenverarbeitung ist unrechtmäßig, jedoch verlangt die betroffene Person die Nutzungseinschränkung anstelle einer Löschung der personenbezogenen Daten
  - Die personenbezogenen Daten werden vom Verantwortlichen für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
  - Die Betroffene/ der Betroffene hat gegen die Verarbeitung Widerspruch eingelegt. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche den Widerspruch überprüft.
2. Nach einer wirksamen Einschränkung der Verarbeitung dürfen die betreffenden personenbezogenen Daten nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutze Rechte anderer oder aufgrund eines wichtigen öffentlichen Interesses verarbeitet werden.

## 10.5 Recht auf Datenübertragbarkeit, Art. 20 DSGVO

Sofern die Datenverarbeitung auf einer Einwilligung beruht oder zur Durchführung eines Vertrages erforderlich war, hat die Betroffene/der Betroffene das Recht die sie/ihn betreffenden personenbezogenen Daten zu erhalten und an einen anderen Verantwortlichen zu übermitteln, soweit dies technisch möglich ist.

## 10.6 Recht auf Widerspruch, Art. 21 DSGVO

Die betroffene Person hat jederzeit das Recht gegen die Datenverarbeitung Widerspruch einzulegen, die auf einer Einwilligung beruht oder zur Wahrung berechtigter Interessen erforderlich ist. Dafür muss das Ergebnis einer Abwägung ergeben, dass das aufgrund einer besonderen Situation ergebende, schutzwürdige Interesse der Betroffenen/des Betroffenen das Interesse des Unternehmens an der Verarbeitung überwiegt. Ein Widerspruchsrecht besteht nicht, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

## 10.7 Recht auf Aufsichtsbeschwerde, Art. 77 DSGVO i.V.M. § 19 BDSG

Darüber hinaus steht der betroffenen Person das Recht zu, eine Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen, wenn sie der Auffassung ist, dass die Verarbeitung ihrer personenbezogenen Daten unrechtmäßig erfolgt ist.

# 11 Vertraulichkeit der Datenverarbeitung

Alle Mitarbeiterinnen und Mitarbeiter der DS-Gruppe unterliegen der Pflicht den Datenschutz einzuhalten („Datengeheimnis“). Eine unbefugte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist untersagt.

1. Alle Mitarbeiterinnen und Mitarbeiter müssen sich vor Beginn ihrer Tätigkeit schriftlich zur Vertraulichkeit verpflichten. Die entsprechenden Muster sind über die Personalabteilung der Diersch & Schröder GmbH & Co. KG erhältlich. Dabei ist zu versichern, dass die im Rahmen der Tätigkeit erlangten personenbezogenen Daten nicht für private oder wirtschaftliche Interessen genutzt, an Unbefugte weitergeleitet oder in sonstiger Weise zugänglich gemacht werden. Diese Pflicht besteht über das Ende des Beschäftigungsverhältnisses hinaus.
2. Um ein hohes Maß an Vertraulichkeit zu gewährleisten, darf den Mitarbeiterinnen und Mitarbeitern Zugang zu personenbezogenen Daten nur in dem Umfang eingeräumt werden, der konkret zur Erfüllung ihrer Tätigkeiten notwendig ist („Need-to-know-Prinzip“).

## 12 Datensicherheit und Fortbildungen

1. Der Schutz von personenbezogenen Daten vor unbefugten Zugriff, unrechtmäßige Verarbeitung oder unberechtigten Verlust, Veränderung oder Zerstörung ist sicherzustellen. Dafür sind wirksame technisch-organisatorische Maßnahmen in einem Sicherheitskonzept zusammenzustellen, das dem aktuellen Stand der Technik, den verarbeitungsspezifischen Risiken und der Schutzbedürftigkeit der verarbeiteten Daten entspricht.
2. Diese Maßnahmen sind auch vor jeder Einführung neuer IT-Systeme zur Datenverarbeitung zu beachten.
3. Das Sicherheitskonzept soll kontinuierlich überprüft und an die technisch-organisatorischen Änderungen und Entwicklungen zum Schutz von personenbezogenen Daten angepasst werden.
4. Um ein hohes Datenschutzniveau im Unternehmen aufrechtzuerhalten, sind diejenigen Mitarbeiterinnen und Mitarbeiter im erforderlichen Umfang über datenschutzrechtlichen Anforderungen fortzubilden, die regelmäßig oder fortlaufend personenbezogene Daten verarbeiten oder Zugang zu solchen haben.



## 13 Datenschutzkontrolle

1. Für die Gewährleistung eines angemessenen Schutzniveaus und die Konformität mit den geltenden Datenschutzbestimmungen wird regelmäßig die Einhaltung dieser Richtlinie überprüft. Die Kontrolle obliegt dem Compliance Officer der DS-Gruppe, dem Datenschutzbeauftragten oder einem mit Auditrechten beauftragten Prüfern. Die Ergebnisse des Audits sind zu dokumentieren.
2. Eine Datenschutzkontrolle ist erfolgreich beendet, wenn bei allen dokumentierten Mängeln durch die Implementierung geeigneter Maßnahmen Abhilfe geschaffen wurde. Dies ist entsprechend zu überprüfen.

## 14 Datenschutzvorfälle und Rechtsfolgen von Regelverstößen

1. Im Falle eines Datenschutzvorfalls, einem Verstoß gegen diese Richtlinie oder gegen andere Regelungen zum Schutz personenbezogener Daten ist der/ die verantwortliche Mitarbeiter/Mitarbeiterin verpflichtet, den Datenschutzvorfall umgehend seinem/ihrer Vorgesetzten, dem Compliance Officer der DS-Gruppe sowie dem Datenschutzbeauftragten unter **[datenschutz@ds-bremen.de](mailto:datenschutz@ds-bremen.de)** zu melden. Dabei ist über alle zur Sachverhaltsaufklärung notwendigen Informationen zu unterrichten, vorwiegend über den Empfänger, die konkret betroffenen personenbezogenen Daten und die Art und der Umfang der vom Vorfall betroffenen Daten.
2. Besteht für den jeweiligen Datenschutzvorfall eine Meldepflicht gegenüber den Aufsichtsbehörden, hat der Datenschutzbeauftragte diese umgehend zu erfüllen.
3. Wurde ein Datenschutzvorfall, ein Verstoß gegen diese Richtlinie oder ein Verstoß gegen andere datenschutzrechtliche Bestimmungen fahrlässig oder vorsätzlich verursacht, zieht dies arbeitsrechtliche Konsequenzen nach sich, eine fristlose oder ordentliche Kündigung einbegriffen. Daneben können strafrechtliche und zivilrechtliche Sanktionen in Erwägung gezogen werden, etwa die Geltendmachung von Schadensersatzansprüchen.



### Wichtige Information

Diese Datenschutzrichtlinie kann nicht auf alle Fragen und Situationen konkrete Antworten geben. Sind weitere Informationen erforderlich, ist der Compliance Officer unter **[compliance@ds-bremen.de](mailto:compliance@ds-bremen.de)** jederzeit ansprechbar.

## Anlage 1

**Personenbezogene Daten (vgl. Art. 4 Nr. 1 DSGVO)** sind alle Informationen über eine natürliche Person, durch die sie direkt oder indirekt identifiziert wird oder identifizierbar ist. Identifizierbar ist eine Person, sobald zu ihr eine Verbindung mittels personenbezogener Daten hergestellt werden kann, beispielsweise durch Zuordnung einer Kennung, Standortdaten, oder eines oder mehrerer besonderen Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind. Dies ist auch dann der Fall, wenn ein Rückschluss auf eine natürliche Person durch eine Kombination von Informationen – wenn auch erst mit zufälligem Zusatzwissen verknüpft – möglich ist. Unter personenbezogenen Daten fallen insbesondere der Name, die Adresse, die Telefonnummer, die private E-Mail-Adresse, oder Fotos und Videoaufzeichnungen der natürlichen Person sowie Kunden- und Personaldaten. Eine Identifizierung der Person kann mit Hilfe einer Anonymisierung oder Pseudonymisierung ausgeschlossen werden.

**Besonders schutzwürdige personenbezogene Daten** sind alle Informationen über die rassische und ethnische Herkunft, über religiöse oder weltanschauliche Überzeugungen, über politische Meinungen, über eine Gewerkschaftszugehörigkeit, über die Gesundheit oder über die sexuelle Orientierung bzw. das Sexualleben einer betroffenen Person.

Unter einem **Betroffenen** versteht man jede natürliche Person, über die personenbezogene Daten verarbeitet werden.

**Die Verarbeitung personenbezogener Daten (vgl. Art. 4 Nr. 2 DSGVO)** bezeichnet 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, Verarbeitung oder in einer anderen Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die **Einschränkung der Verarbeitung (vgl. Art. 4 Nr. 3 DSGVO)** ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

**Die Übermittlung** ist jede Bekanntgabe von personenbezogenen Daten durch den Verantwortlichen an Dritte.

Das **Profiling (Art. 4 Nr. 4 DSGVO)** bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung,

wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

**Anonymisierung** meint die Verarbeitung von personenbezogenen Daten in der Gestalt, dass ein Personenbezug auf Dauer nicht mehr hergestellt werden kann oder der Rückschluss auf eine natürliche Person nur mit unverhältnismäßigem Aufwand möglich ist.

**Pseudonymisierung (Art. 4 Nr. 5 DSGVO)** ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

**Dateisystem (Art. 4 Nr. 6 DSGVO)** ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

**Verantwortlicher (Art. 4 Nr. 7 DSGVO)** bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

**Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO)** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

**Empfänger (Art. 4 Nr. 9 DSGVO)** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

**Dritter (Art. 4 Nr. 10 DSGVO)** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem



Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

**Einwilligung (Art. 4 Nr. 11 DSGVO)** der betroffenen Person bezeichnet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

**Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO)** ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

**Gesundheitsdaten (Art. 4 Nr. 15 DSGVO)** sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

**Unternehmen (Art. 4 Nr. 18 DSGVO)** ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

**Unternehmensgruppe (Art. 4 Nr. 19 DSGVO)** ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

**Datenschutzvorfall** bezeichnet alle Umstände, die den Verdacht begründen, dass personenbezogene Daten rechtswidrig durch Mitarbeiter oder Dritte erhoben, übermittelt, kopiert, genutzt oder ausgespäht wurden.



# ENERGIE

Gemeinsam besser für **Mobilität**,  
**Wärme** und **Strom** – das treibt uns an.

# CHEMIE

Unsere **Additive** schmieren industrielle  
Produktionsanlagen und schützen Bananenpflanzen.

# YOUNG BUSINESS

Start-ups helfen der DS-Gruppe, **jung** und **innovativ** zu bleiben.