



Gefahrstoffberatung Schnurbusch GmbH & Co. KG

Karen Schnurbusch-Beteiligungs GmbH

## Vereinbarung zwischen gemeinsam Verantwortlichen

zwischen	und	und	und
<b>Chemical Check GmbH</b>	<b>REACH Registration of Chemicals GmbH</b>	<b>Gefahrstoffberatung Schnurbusch GmbH &amp; Co. KG</b>	<b>Karen Schnurbusch-Beteiligungs GmbH</b>
<b>Chemical Check Platz 1-7 32839 Steinheim</b>	<b>Chemical Check Platz 1-7 32839 Steinheim</b>	<b>Chemical Check Platz 1-7 32839 Steinheim</b>	<b>Chemical Check Platz 1-7 32839 Steinheim</b>
<b>- Chemical Check genannt-</b>	<b>- REACH genannt -</b>	<b>- Gefahrstoffberatung Schnurbusch-</b>	<b>-K. Schnurbusch Bet. genannt-</b>

- gemeinsam nachfolgend „Parteien“ genannt –

### 1 Vertragsgegenstand

- 1.1 Dieser Vertrag stellt eine Vereinbarung gemäß Art. 26 Datenschutzgrundverordnung (DSGVO) zur Regelung einer Verarbeitung personenbezogener Daten in gemeinsamer Verantwortlichkeit der Parteien dar.
- 1.2 Die Zusammenarbeit der Parteien - nachfolgend als „Zusammenarbeit“ bezeichnet – bringt es mit sich, dass die Parteien gemeinsam die Zwecke und/oder wesentliche Elemente der Mittel der Verarbeitung bestimmter personenbezogener Daten bestimmen (nachfolgend als „Daten“ oder „Datenverarbeitung“ bezeichnet). Die Parteien fungieren deshalb im datenschutzrechtlichen Sinn als gemeinsam Verantwortliche i.S.v. Art. 26 in Verbindung mit Art. 4 Nr. 7 DSGVO.
- 1.3 Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung der Zusammenarbeit und konkretisiert insbesondere die Verteilung und Erfüllung der Aufgaben und Pflichten nach anwendbarem Datenschutzrecht (insbesondere der DSGVO) zwischen den Parteien im Hinblick auf die Datenverarbeitung.

### 2 Gegenstand, Zweck, Mittel und Umfang der Datenverarbeitung

- 2.1 Gegenstand der Datenverarbeitung ist der gemeinsame Betrieb eines CRM-Systems (Kundenpflege-Systems) sowie der IT-Infrastruktur, wie im Einzelnen im Anhang beschrieben.
- 2.2 Die Datenverarbeitung erfolgt entsprechend den in Anlage 1 zu diesem Vertrag enthaltenen Festlegungen zu Zwecken, Mitteln und Umfang. Sie bezieht sich auf die in Anlage 1 spezifizierte Art der Daten und die dort bestimmten Kategorien betroffener Personen.
- 2.3 In Anlage 1 zu diesem Vertrag ist darüber hinaus abschließend festgelegt, welche Partei oder ob die Parteien gemeinsam (jeweils) die Kategorien betroffener Personen, die Art der personenbezogenen Daten, die Mittel und Zwecke der Verarbeitung bestimmt haben.
- 2.4 Die Parteien sind sich einig, dass die Datenverarbeitung ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) stattfindet. Jede Verlagerung in ein Drittland muss zwischen den Parteien abgestimmt werden und darf generell nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44ff. DSGVO erfüllt sind.

### **3 Phasen der Datenverarbeitung/Zuständigkeiten und Verantwortung**

- 3.1 Die Zuständigkeiten im Hinblick auf die gemeinsame Datenverarbeitung sind zwischen den Parteien nach Phasen der Datenverarbeitung folgendermaßen aufgeteilt:
- Für die Erhebung der Daten sind alle Vertragsparteien zuständig.
  - Für die Speicherung der Daten ist Vertragspartei Chemical Check zuständig.
  - Für die Änderung und Löschung der Daten, die Einschränkung deren Verarbeitung und deren Übertragung nach Art. 20 DSGVO ist Vertragspartei Chemical Check zuständig.
  - Für die sonstigen Verarbeitungen sind alle Vertragsparteien zuständig.
- Die Parteien dürfen die Daten für die in diesem Vertrag festgelegten Zwecke verwenden.
- 3.2 Die Daten sind in einem strukturierten, gängigen und maschinenlesbaren Format zu speichern.
- 3.3 Vor einer etwaigen Löschung von Daten sind zuvor die anderen Parteien zu informieren; sie dürfen der Löschung aus berechtigtem Grund widersprechen, etwa sofern sie eine gesetzliche Aufbewahrungspflicht trifft. Die Parteien haben ein Protokoll über die Löschung bzw. Vernichtung der Daten zu erstellen.
- 3.4 Die Parteien haben eigenständig dafür Sorge zu tragen, dass sie sämtliche, in Bezug auf die Daten bestehende, gesetzliche Aufbewahrungspflichten einhalten können. Sie haben hierzu (unbeschadet entsprechender Regelungen in diesem Vertrag) angemessene Datensicherungsvorkehrungen zu treffen. Dies gilt insbesondere im Falle einer Beendigung der Zusammenarbeit.
- 3.5 Die Parteien sind ungeachtet der unter Ziffer 3.1 getroffenen Festlegungen bezüglich der ihnen jeweils einzeln zugeteilten Zuständigkeiten für bestimmte Phasen der Datenverarbeitung gemeinsam für die Rechtmäßigkeit aller Verarbeitungen verantwortlich.

### **4 Information der betroffenen Personen**

- 4.1 Alle Vertragsparteien haben die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO sicherzustellen.
- 4.2 Betroffenen Personen sind die erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen. Die Parteien werden sich auf Inhalt und Formulierung dieser Informationen verständigen.
- 4.3 Chemical Check hat die wesentlichen Inhalte dieses Vertrages den Betroffenen entsprechend Art. 26 Abs. 2 Satz 2 DSGVO zur Verfügung zu stellen; die Parteien werden sich auf Inhalt und Formulierung dieser Informationen verständigen.

### **5 Erfüllung der sonstigen Rechte der betroffenen Personen**

- 5.1 Vertragspartei Chemical Check ist für die Bearbeitung und Beantwortung von Anträgen auf Wahrnehmung der sonstigen nach den Art. 15 ff. DSGVO bestehenden Rechte der betroffenen Personen („Betroffenenrechte“) zuständig.
- 5.2 Ungeachtet der Regelung in Ziffer 5.1 dieses Vertrags stimmen die Parteien überein, dass sich betroffene Personen an alle Parteien zwecks Wahrnehmung der ihnen jeweils zustehenden Betroffenenrechte wenden können. In einem solchen Fall ist die in Anspruch genommene

Partei dazu verpflichtet, das Ersuchen eines Betroffenen an Chemical Check unverzüglich weiterzuleiten. Die Parteien verständigen sich über die Beantwortung und Bearbeitung der Anfrage.

- 5.3 Im Falle eines Betroffenenersuchens auf Löschung findet Ziffer 3.3 dieses Vertrags entsprechende Anwendung.

## 6 **Sicherheit der Verarbeitung**

- 6.1 Die Parteien haben vor Beginn der Verarbeitung die in Anlage 2 dieses Vertrags spezifizierten technischen und organisatorischen Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten.
- 6.2 Die technischen und organisatorischen Maßnahmen sind für alle Vertragsparteien identisch. Bei zukünftigen Änderungen verständigen sich die Parteien.
- 6.3 Die Parteien gewährleisten, alle geeigneten technischen und organisatorischen Maßnahmen so durchzuführen, dass die Datenverarbeitung im Einklang mit den Anforderungen anwendbarer Datenschutzbestimmungen (insbesondere der DSGVO) erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

## 7 **Einschaltung von Auftragsverarbeitern**

- 7.1 Jede Partei darf Auftragsverarbeiter im Rahmen der gemeinsamen Datenverarbeitung nur nach vorheriger Zustimmung der anderen Parteien einschalten.
- 7.2 Zur Prüfung einer solchen Zustimmung hat die beauftragungswillige Partei den anderen Parteien eine Kopie der abzuschließenden Vereinbarung zur Auftragsverarbeitung zur Verfügung zu stellen.
- 7.3 Die Vereinbarung hat den Anforderungen der Art. 28, 29 DSGVO zu entsprechen. Die Parteien müssen die Vereinbarung als Auftraggeber wirksam abschließen. Jede Partei kann sich von den anderen Parteien dabei vertreten lassen.
- 7.4 Sofern ein außerhalb der EU ansässiger Auftragsverarbeiter eingeschaltet werden soll, findet Ziffer 2.4 dieses Vertrags entsprechende Anwendung.
- 7.5 Eingeschaltete Auftragsverarbeiter sind von der jeweils beauftragungswilligen Partei regelmäßig in geeigneter Form zu überprüfen.
- 7.6 Die Parteien werden sich je zugestimmter Auftragsverarbeitung über deren jeweilige Durchführung, insbesondere hinsichtlich der Weisungserteilung gegenüber dem jeweiligen Auftragsverarbeiter sowie dessen Überprüfung im gegenseitigen Benehmen nach Treu und Glauben verständigen.

## 8 **Vorgehen bei Datenschutzverletzungen**

- 8.1 Vertragspartei Chemical Check ist für die Prüfung und Bearbeitung aller Verletzungen des Schutzes personenbezogener Daten i.S.v. Art. 4 Nr. 12 DSGVO (nachfolgend als „Datenpanne(n)“ bezeichnet) einschließlich der Erfüllung aller deshalb etwaig bestehender Meldepflichten gegenüber der zuständigen Aufsichtsbehörde nach Art. 33 DSGVO oder gegenüber betroffenen Personen nach Art. 34 DSGVO zuständig.
- 8.2 Die Parteien werden jede etwaig festgestellte Datenpanne unverzüglich den anderen Parteien anzeigen und bei einer etwaigen Meldung nach Art. 33, 34 DSGVO sowie einer Aufklärung und

Beseitigung von Datenpannen im Rahmen des Erforderlichen und Zumutbaren mitwirken, insbesondere sämtliche in diesem Zusammenhang relevanten Informationen einander unverzüglich zur Verfügung stellen.

- 8.3 Bevor Chemical Check eine Meldung nach Ziffer 8.1 dieses Vertrags an eine Aufsichtsbehörde oder eine betroffene Person vornimmt, stimmt sie das Vorgehen mit den anderen Parteien ab.

## 9 **Sonstige gemeinsame und gegenseitige Pflichten**

- 9.1 Die Parteien haben alle mit der Datenverarbeitung beschäftigten Personen schriftlich zur Wahrung der Vertraulichkeit im Hinblick auf die Daten zu verpflichten.
- 9.2 Alle Vertragsparteien haben sich gegenseitig unverzüglich und vollständig zu informieren, wenn Fehler oder Unregelmäßigkeiten bei der Datenverarbeitung oder Verletzungen von Bestimmungen dieses Vertrags oder anwendbaren Datenschutzrechts (insbesondere der DSGVO) festgestellt werden.
- 9.3 Für die Parteien gilt die jeweilige Geschäftsführung als Ansprechpartner.
- 9.4 Die Parteien werden sich bei der Einhaltung der in diesem Vertrag vereinbarten Festlegungen sowie anwendbaren gesetzlichen Datenschutzbestimmungen (insbesondere der DSGVO) im Rahmen des Erforderlichen und Zumutbaren gegenseitig unterstützen; hierzu zählen insbesondere:
- Die Verpflichtung, die jeweils andere Partei bei der Etablierung und Aufrechterhaltung angemessener technischer und organisatorischer Maßnahmen gemäß Ziffer 6 dieses Vertrags zu unterstützen;
  - die Verpflichtung, sich gegenseitig bei einer etwaig erforderlichen Datenschutz-Folgenabschätzung und etwaigen Konsultationspflichten der zuständigen Aufsichtsbehörde gemäß Art. 35, 36 DSGVO zu unterstützen;
  - die Verpflichtung, sich bei der Einrichtung und Pflege der beiderseitigen Verzeichnisse der Verarbeitungstätigkeiten zu unterstützen.
- 9.5 Die Parteien verpflichten sich, alle im Zusammenhang mit diesem Vertrag, der Zusammenarbeit oder der Datenverarbeitung stehenden Fakten, Auswirkungen und ergriffenen Maßnahmen zu dokumentieren.

## 10 **Zusammenarbeit mit Aufsichtsbehörden**

- 10.1 Die Parteien werden sich gegenseitig unverzüglich anzeigen, wenn sich eine Datenschutzaufsichtsbehörde im Zusammenhang mit diesem Vertrag, der Zusammenarbeit oder der Datenverarbeitung an sie wendet.
- 10.2 Die Parteien sind sich darüber einig, dass Aufforderungen zuständiger Datenschutzaufsichtsbehörden grundsätzlich Folge zu leisten ist, insbesondere sind etwaig angeforderte Informationen zu überlassen und Möglichkeiten zur Prüfung (auch vor Ort) einzuräumen. Die Parteien gewähren zuständigen Datenschutzaufsichtsbehörden in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.
- 10.3 Soweit wie möglich werden sich die Parteien im gegenseitigen Benehmen miteinander abstimmen, bevor etwaigen Anfragen von zuständigen Datenschutzaufsichtsbehörden Folge geleistet wird bzw. Informationen im Zusammenhang mit diesem Vertrag, der Zusammenarbeit oder der Datenverarbeitung an zuständige Datenschutzaufsichtsbehörden herausgegeben werden.

Gefahrstoffberatung Schnurbusch GmbH & Co. KG

Karen Schnurbusch-Beteiligungs GmbH

**11 Haftung**

11.1 Die Parteien haften gegenüber betroffenen Personen nach den gesetzlichen Vorschriften.


**12 Schlussbestimmungen**

12.1 Die Laufzeit der Vereinbarung ist unbeschränkt. Jede Partei kann die Vereinbarung mit einer Frist von einem Monat kündigen.

12.2 Es gilt deutsches Recht einschließlich der DSGVO. Gerichtsstand ist Steinheim.


Steinheim, 06.03.2019

Ort, Datum

  
L. Jocke  
Chemical Check GmbH

Steinheim, 06.03.2019

Ort, Datum

  
REACH Registration of Chemicals GmbH


Steinheim, 06.03.2019

Ort, Datum

  
Gefahrstoffberatung Schnurbusch  
GmbH & Co. KG

Steinheim, 06.03.2019

Ort, Datum

  
Karen Schnurbusch Beteiligungs GmbH

### Anlage 1

- Zwecke, Mittel und Umfang der Datenverarbeitung.
  - Art der Daten und die Kategorien betroffener Personen.
  - Festlegung, welche Partei oder ob beide Parteien gemeinsam (jeweils) die Kategorien betroffener Personen, die Art der personenbezogenen Daten, die Mittel und Zwecke der Verarbeitung bestimmt haben.
- 
- Zwecke der Datenverarbeitung  
Die gemeinsame Datenverarbeitung erfolgt aus dem berechtigten Interesse der Parteien, eine effektive Umsetzung der Vertragsabläufe zwischen den einzelnen Unternehmen und im Zusammenhang mit gemeinsamen Kunden und Vertragspartnern zu gewährleisten. Auch zur effektiven Mitarbeiterkommunikation und -organisation der einzelnen Parteien wird ein gemeinsames IT-System genutzt.
- 
- Mittel der Datenverarbeitung  
Die gemeinsame Datenverarbeitung erfolgt mittels des möglichen Zugriffs jeder Partei auf die gemeinsam genutzte IT-Struktur.
- 
- Umfang der Datenverarbeitung  
Erheben, Erfassen, Organisation, Ordnen, Speicherung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Einschränkung, Löschen, Vernichtung
- 
- Art der personenbezogenen Daten  
Mitarbeiterdaten, Kundendaten, Vertragspartnerdaten, Bewerberdaten
- 
- Kategorien der betroffenen Personen  
Mitarbeiter, Kunden, Vertragspartner, Bewerber

## Anlage 2

### **Technische und organisatorische Maßnahmen (TOMs) der Chemical Check-Firmengruppe zu Datenschutz und Datensicherheit gemäß Bundesdatenschutzgesetz (BDSG) und Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)**

#### **1. Zutrittskontrolle**

Maßnahmen, die geeignet sind, Unbefugten Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

- Sichtkontrollen und Zutrittskontrolle durch Türöffner mit Gegensprechanlage
- Alarmanlage mit Innenraumüberwachung
- Alarmanlagen-Schließsystem mit Codesperre
- Alarmgesicherte Fenster inklusive bruchsicke Glas
- Manuelles Schließsystem
- Videoüberwachung des Gebäudeumfelds (nicht öffentlicher Bereich)
- Personenkontrolle beim Empfang von Besuchern
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal

Ausgaberegulierung Schlüssel:

Schlüssel werden ausschließlich personenbezogen ausgegeben und protokolliert.

Die Serverräume sind stets verschlossen. Sie liegen in einem der Brandabschnitte nach Brandschutzkonzept. Die Schlüsselausgabe erfolgt nur an einen eingeschränkten Personenkreis und wird protokolliert. Unternehmensfremden Personen, wie Wartungstechnikern, werden Begleitpersonen an die Seite gestellt. Reinigungspersonal hat keinen Zutritt zu den Serverräumen.

#### **2. Zugangskontrolle / Absicherung Systemzugang**

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Für die IT-Systeme werden Administratoren eingesetzt. Diese nutzen spezielle Passwortkonventionen. Die Administratorenarbeit wird systemseitig protokolliert.

- Es werden individuelle, persönliche Benutzerkennungen angewendet.
- Es existiert eine systemseitige und mittels Arbeitsanweisung festgelegte Passwortregelung. Es werden mindestens 8 Zeichen und ein entsprechender Zeichenmix verwendet.
- Es gibt eine systemseitige Zugangssperre bei mehr als 3 Anmeldeversuchen.
- Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert.
- Zuordnung von Benutzerrechten
- Einsatz einer 2-stufigen Hardware/ Firewall-Struktur (redundant)

- Einsatz einer selbstlernenden Anti-Viren-Software
- Einsatz von VPN-Technologie (Fernzugriff)
- Es werden regelmäßig Updates und Sicherheitspatches installiert, um das Schutzniveau hoch zu halten.
- Externe Schnittstellen (USB, etc) sind gesperrt
- Interne Datenträger (wie USB-Sticks) unterliegen der Freigabe durch den Administrator.

### **3. Zugriffskontrolle**

Es existiert ein Berechtigungskonzept (verschiedene Berechtigungsstufen) für die Zugriffe der Mitarbeiter auf Daten. Die Rechteverwaltung erfolgt durch Administratoren. Die Anzahl der Administratoren ist auf ein Minimum beschränkt.

- Einsatz einer 2-stufigen Hardware/ Firewall-Struktur (redundant)
- Einsatz einer selbstlernenden Anti-Viren-Software
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern
- Es erfolgt eine organisatorische Trennung von Administration und Betrieb/Anwendung.
- Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert.
- Physische Löschung von Datenträgern vor Wiederverwendung

### **4. Trennungskontrolle**

Es erfolgt eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden sowie eine physisch getrennte Speicherung auf gesonderten physikalischen oder virtuellen System oder Datenträgern. Es erfolgt eine Trennung von Produktiv- und Testsystemen.

### **5. Weitergabekontrolle**

Die Weitergabekontrolle beim Datentransfer unterbindet das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei elektronischen Übertragungen oder Transporten.

Zu diesem Zweck sind Standleitungen bzw. VPN-Tunnel eingerichtet. Datenübermittlungen werden standardmäßig via https oder SFTP durchgeführt. E-Mails mit sensiblen Daten werden verschlüsselt versandt. Externe Datenträger wie z.B. CDs, USB-Sticks etc. werden vor Weitergabe verschlüsselt.

### **6. Eingabekontrolle**

Protokollierung der Eingabe, Änderung und Löschung von Daten

Die Rechte zur Eingabe, Änderung und Löschung von Daten werden auf Basis eines Berechtigungskonzeptes vergeben. Die Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen von Daten wird durch individuelle Benutzernamen (nicht Benutzergruppen) gewährleistet.



## 7. Verfügbarkeit und Belastbarkeit

Die Daten werden vor zufälliger Zerstörung und Verlust folgendermaßen geschützt:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in den Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlage
- Feuerlöscher in den Serverräumen
- Aufbewahrung von Datensicherungen an einem sicherem ausgelagertem Ort
- Erstellung eines Backup- und Recoverykonzeptes
- Erstellung eines Notfallplans
- Serverräume nicht unter Sanitäreinrichtungen
- Regelmäßige Sicherung von Systemzuständen
- Regelmäßige Sicherung von Dateibeständen
- Regelmäßige Sicherung von Datenbanken

Der Brandschutz wird sichergestellt durch ein komplettes Brandschutzkonzept inkl. der Einrichtungen

- Brandschutztüren
- lokale Feuerlöscher
- Brand- bzw. Rauchmelder
- Lokale Löschdecken

Eine rasche Wiederherstellbarkeit der Systeme wird anhand eines Backup- und Recoverykonzeptes gewährleistet. Weiterhin wird regelmäßig die Wiederherstellung von Daten getestet.

## 8. Auftragskontrolle

Die Auswahl der Auftragnehmer erfolgt unter Sorgfaltsgesichtspunkten (Verschwiegenheitserklärung/ Auftragsdatenverarbeitungsvereinbarung).

## 9. Pseudonymisierung

Ist auf Grund der Leistungsart nicht erforderlich und nicht gegeben.

## 10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer verpflichtet sich, gemäß der DSGVO besonders sorgsam mit persönlichen Daten umzugehen. Etwaige zukünftige Mitarbeiter oder beauftragte Dritte werden durch den Auftragnehmer ebenfalls zur Einhaltung des Datenschutzes aufgefordert.

Dem Auftragnehmer ist es wichtig sein Datenschutzmanagement kontinuierlich zu verbessern und Maßnahmen zur Sensibilisierung und Aufrechterhaltung des Datenschutzes zu treffen. Er bemüht sich die erforderlichen Dokumente zu pflegen und sorgsam zu verwalten.