

## Vertrag für die Auftragsdatenverarbeitung

zwischen

**Niedersächsisches Ministerium für Inneres und Sport (auch mit Wirkung und Gültigkeit für den kommunalen Bereich)**

Lavesallee 630169, Hannover

(„Auftraggeber“)

und

**Dräger Safety AG & Co. KGaA**

Revalstraße 1

23560 Lübeck

(„Auftragnehmer“)

(Auftragnehmer und Auftraggeber nachfolgend jeweils auch „Partei“ und zusammen „Parteien“)

Der Gegenstand dieses Vertrages ist die datenschutzgerechte Erledigung der im Auftrage AZ 02081-408 14 vom 31.07.2015 („Hauptvertrag“) vereinbarten Leistungen.

Die nachfolgend enthaltenen Verweise auf Artikel der „EU Datenschutzrichtlinie“<sup>1</sup> oder der „EU Datenschutzrichtlinie für elektronische Kommunikation“<sup>2</sup>, die von allen Mitgliedsstaaten der EU in nationales Recht umzusetzen sind, beziehen sich dabei immer auch die auf die jeweilige Umsetzung des Artikels in nationales Recht.

Die Parteien treffen hierzu nachfolgende Vereinbarungen:

### 1. Anwendungsbereich

Der Auftragnehmer ist vom Auftraggeber mit der Erbringung von Leistungen für den Gesamtbe-

---

<sup>1</sup> Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

<sup>2</sup> Gemeint ist die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, in der durch die Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz entstandene Fassung. Die entsprechenden Änderungen wurden in Deutschland vor allem durch die Reform des BDSG in 2009, aber auch durch die Reform des Telekommunikationsgesetzes (TKG) 2010 umgesetzt.

reich Datenverarbeitung, Wartung von IT-Infrastruktur und Fernwartung über Telekommunikationsleitungen beauftragt. Dabei ist nicht auszuschließen, dass der Auftragnehmer im Zuge der vertragsgemäßen Durchführung der Leistungen die Möglichkeit des Zugriffs auf personenbezogene Daten im Sinne von Artikel 2 der EU Datenschutzrichtlinie<sup>3</sup>, die vom Auftraggeber oder aus der Sphäre des Auftraggebers stammen (nachfolgend: „Auftraggeberdaten“), verwenden muss.

Dieser Vertrag zum Datenschutz enthält die dabei zu beachtenden allgemeinen Anforderungen und gilt für alle Datenverarbeitungsaufträge des Auftraggebers an den Auftragnehmer und ergänzt und konkretisiert die Regelungen zum Datenschutz im Hauptvertrag.

## 2. Pflichten des Auftragnehmers

- 2.1 Der Auftragnehmer beachtet bei der Verarbeitung von Auftraggeberdaten die am Sitz des Auftraggebers geltenden Datenschutzgesetze, die am Sitz des Auftragnehmers geltenden Datenschutzgesetze und in jedem Fall mindestens die Anforderungen, die sich aus der EU Datenschutzrichtlinie und der EU Datenschutzrichtlinie für elektronische Kommunikation (nachfolgend: „anwendbare Datenschutzgesetze“) ergeben. Dies gilt nur, soweit nicht gesetzlich zwingend der Vorrang eines bestimmten Datenschutzgesetzes angeordnet ist.

Der Auftragnehmer hat die innerbetriebliche Organisation so gestaltet, dass sie den Anforderungen der anwendbaren Datenschutzgesetze jederzeit gerecht wird.

Der Auftragnehmer verarbeitet und nutzt Auftraggeberdaten nur im Rahmen des Auftrags und entsprechend den Weisungen des Auftraggebers. Der Auftraggeber ist und bleibt als speichernde und verantwortliche Stelle der „Herr der Daten“. Eine Berichtigung, Löschung und Sperrung von Auftraggeberdaten erfolgt ausschließlich auf Weisung des Auftraggebers.

- 2.2 Die Verarbeitung der Auftraggeberdaten darf nicht zu einer inhaltlichen Umgestaltung führen, auch wenn es sich um die Bereinigung von Fehlern handelt. Zulässig ist nur die Bereinigung rein technisch bedingter Fehler. Inhaltliche Änderungen der Auftraggeberdaten sind nur mit Einwilligung des Auftraggebers, die mindestens in Textform erteilt wurde, durchzuführen. Eine Verwendung von Auftraggeberdaten in anonymisierter Form für statistische Zwecke oder zur Qualitätsüberwachung der Leistungen des Auftragnehmers ist ausdrücklich gestattet.
- 2.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen anwendbare Datenschutzgesetze verstößt, weist der Auftragnehmer den Auftraggeber in Textform (z.B. E-Mail) darauf hin. Der Auftragnehmer unterrichtet den Auftraggeber auf dem gleichen Weg bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder bei anderen wesentlichen Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten. Ebenso wird der Auftragnehmer Verstöße gegen Weisungen des Auftraggebers unaufgefordert anzeigen.
- 2.4 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 5 NDSG zu wahren.
- 2.5 Die Einschaltung von Subunternehmen ist ausgeschlossen. Die Beauftragung von Subunternehmen mit der Verarbeitung von personenbezogenen Daten ist in keinem Fall zulässig.
- 2.6 Der Auftragnehmer ist zur Beauftragung von Subunternehmern bzw. Unterauftragsdatenverarbeitern nur mit schriftlicher Zustimmung des Auftraggebers berechtigt. Werden Subunternehmer

<sup>3</sup> In Deutschland: § 3 Nr. 1 BDSG

bzw. Unterauftragsdatenverarbeiter eingesetzt, gewährleistet der Auftragnehmer die vertragliche Absicherung des Datenschutzes auf dem durch diese Vereinbarung festgelegten Niveau. Bereits mit Abschluss dieser Vereinbarung wird dem Auftragnehmer eine widerrufliche Genehmigung für den Einsatz der in Anlage 6 – Subunternehmer – aufgeführten Subunternehmer erteilt.

- 2.7 Die Parteien teilen einander die Kontaktdaten des jeweiligen betrieblichen Datenschutzbeauftragten mit oder, wenn kein solcher bestellt wurde, die Kontaktdaten der beim Auftragnehmer für die Einhaltung der anwendbaren Datenschutzgesetze verantwortlichen Person.
- 2.8 Der Auftragnehmer wird nach Abschluss der Vertragsbeziehung alle personenbezogenen Daten zurückgeben oder, nach Absprache mit Auftraggeber, deren Löschung bestätigen
- 2.9 Allgemeine Weisungen des Auftraggebers für den Umgang mit Auftraggeberdaten bedürfen der Textform. Mündliche Weisungen des Auftraggebers im Einzelfall dürfen nur durch hierzu autorisierte Personen erfolgen und müssen wenigstens in Textform bestätigt werden.

### 3. Technisch-organisatorische Maßnahmen

- 3.1 Der Auftragnehmer gewährleistet in der eigenen Sphäre die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen entsprechend Artikel 17 Abs. 1 EU Datenschutzrichtlinie<sup>4</sup> hierzu. Er informiert den Auftraggeber unverzüglich über geplante Veränderungen in der Organisation der Datenverarbeitung und den angewandten Verfahren, soweit sie für die Auftragsdatenverarbeitung sicherheitsrelevant sind. Entsprechendes gilt in Fällen von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Der Auftragnehmer stellt sicher, dass die datenschutzrechtlichen Rahmenbedingungen auch bei Einsatz von Telearbeitsplätzen oder mobilem Zugriff seiner Mitarbeiter auf Datenverarbeitungssysteme oder Daten des Auftragnehmers beachtet werden. Insbesondere ergreift der Auftragnehmer folgende Maßnahmen zur Absicherung der Datenverarbeitungssysteme, mit denen Auftraggeberdaten verarbeitet oder genutzt werden oder von denen aus bestimmungsgemäß ein Zugriff auf solche Daten möglich ist:
  - a.) Zutrittskontrolle: Im Rahmen der Zutrittskontrolle erhalten Betriebsfremde nur in Begleitung von Personal des Auftragnehmers Zugang zu den Geschäftsräumen. Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen verwehrt.
  - b.) Zugangskontrolle: Durch entsprechende Zugangskontrollen wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
  - c.) Zugriffskontrolle: Die zur Benutzung der Datenverarbeitungssysteme Berechtigten können ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen. Kein Dritter darf Zugriff auf die Auftraggeberdaten haben. Der Auftragnehmer gewährleistet, dass Datenträger nicht entwendet oder unbefugt gelesen oder verändert werden.
  - d.) Weitergabekontrolle: Die Auftraggeberdaten werden bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger durch Sicherheitsmaßnahmen davor geschützt, dass sie unbefugt gelesen, kopiert, verändert oder entfernt werden können oder festgestellt werden kann, an welchen Stellen eine Übermittlung von Auftraggeberdaten durch Datenübertragungseinrichtungen vorgesehen ist. Dies erfolgt insbesondere durch die Verwendung einer entsprechende Sicherheitssoftware, Passwörtern und Verschlüsselungstechnologien.

---

<sup>4</sup> In Deutschland: § 9 BDSG und die Anlage hierzu.

- e.) Eingabekontrolle: Es kann festgestellt und überprüft werden, welche Auftraggeberdaten zu welcher Zeit, von wem in das Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.
  - f.) Auftragskontrolle: Der Auftragnehmer hat Vorsorge getroffen, dass Auftraggeberdaten nur entsprechend den Weisungen der Auftraggeber verarbeitet werden.
  - g.) Verfügbarkeitskontrolle: Auftraggeberdaten werden gegen zufällige Zerstörung oder Verlust geschützt. Soweit Auftraggeberdaten bestimmungsgemäß beim Auftragnehmer gespeichert sind, werden in regelmäßigen Abständen Sicherheitskopien der Auftraggeberdaten erstellt.
  - h.) Trennungskontrolle: Der Auftragnehmer speichert und verarbeitet Auftraggeberdaten, die zu unterschiedlichen Zwecken erhoben werden, getrennt voneinander.
- 3.2 Weitere Einzelheiten zu den technisch-organisatorischen Maßnahmen sind in **Anlage 1 – Technisch organisatorische Maßnahmen** festgelegt.

#### 4. Pflichten des Auftraggebers

- 4.1 Der Auftraggeber beurteilt die Zulässigkeit der Verwendung von Auftraggeberdaten durch den Auftragnehmer im Rahmen des Auftrags gemäß den anwendbaren Datenschutzgesetzen. Der Auftraggeber stellt sicher, dass die Auftraggeberdaten zweifelsfrei aus dem Herrschaftsbereich des Auftraggebers stammen und ordnungsgemäß erhoben wurden bzw. werden.
- 4.2 Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses gemäß Art. 18 bis 21 EU Datenschutzrichtlinie<sup>5</sup> liegt beim Auftraggeber.
- 4.3 Der Auftraggeber wird den Auftragnehmer unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten unterrichten, insbesondere bei der Prüfung der Ergebnisse der Auftragsdatenverarbeitung.
- 4.4 Der Auftraggeber wahrt die Rechte von Betroffenen nach Art. 10 bis 12 EU Datenschutzrichtlinie<sup>6</sup> und gibt dem Auftragnehmer entsprechende Anweisungen.
- 4.5 Der Auftraggeber erteilt dem Auftragnehmer unverzüglich die zur Beantwortung von Auskunftsverlangen der Kontrollstelle i.S.d. Art. 28 EU-Datenschutzrichtlinie<sup>7</sup> nötigen Weisungen.
- 4.6 Soweit der Auftraggeber die Auftraggeberdaten selbst als Auftragnehmer eines Dritten verwendet und die Tätigkeit des Auftragnehmers daher eine Unterauftragsdatenverarbeitung darstellt, stellt der Auftraggeber sicher, dass der Dritte "Herr der Daten" und verantwortliche Stelle i.S.d. anwendbaren Datenschutzgesetze bleibt und die ihm nach den anwendbaren Datenschutzgesetzen zustehenden Rechte hat. Der Auftraggeber wird bei mehreren Auftraggebern vertraglich Vorsorge tragen, dass solche Anfragen vom Auftraggeber koordiniert und gesammelt werden und vom Auftraggeber stellvertretend für die Dritten bearbeitet werden. Dies gilt nicht bei konkreten erheblichen Beanstandungen der Dritten, für die der Auftragnehmer verantwortlich ist.
- 4.7 Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei, einschließlich der Kosten der angemessenen Rechtsverteidigung, die in Zusammenhang mit der Auftragsdatenverarbeitung erhoben werden. Im Hauptvertrag vereinbarte Haftungsbeschränkungen gelten insofern

<sup>5</sup> In Deutschland: § 4 g Abs. 2 Satz 2 BDSG.

<sup>6</sup> In Deutschland: §§ 33-35 BDSG.

<sup>7</sup> In Deutschland: Zuständige Datenschutzaufsichtsbehörde, § 38 BDSG.

nicht. Der Freistellungsanspruch besteht nicht, soweit ein Schaden des Dritten seine Ursache in einer schuldhaften Verletzung der Pflichten aus dieser Vereinbarung zum Datenschutz durch den Auftragnehmer hat.

## 5. Besonders geschützte Daten, Patientendaten, Arzt-/Patientengeheimnis

- 5.1 Die Regelungen dieser Ziff. 5 gelten vorrangig für den Umgang mit besonderen Kategorien personenbezogener Daten gemäß Art. 8 Abs. 1 EU-Datenschutzrichtlinie<sup>8</sup>, insbesondere für Gesundheitsdaten, für Patientendaten i.S.d. jeweils einschlägigen Krankenhausgesetzes sowie für alle Daten, die nach den anwendbaren Datenschutzgesetzen unter das Arzt-/Patientengeheimnis fallen („Besondere Auftraggeberdaten“).
- 5.2 Der Auftraggeber wird dafür Sorge tragen, dass der Auftragnehmer bei der Durchführung der vertraglichen Leistungen keinen unberechtigten Zugriff auf besondere Auftraggeberdaten hat. Dazu zählen z.B. Untersuchungsbefunde oder Daten, die diesen Befunden zugrunde liegen. Der Auftraggeber stellt durch geeignete organisatorische und vertragliche Vorkehrungen sicher, dass dem Auftragnehmer ein Zugriff auf solche besonderen Auftraggeberdaten in rechtlich zulässiger Weise möglich ist.
- 5.3 Der Auftraggeber ist verpflichtet, seinen Informationspflichten gegenüber Patienten, wie sie sich z.B. aus dem jeweiligen Krankenhausgesetz ergeben, umfassend nachzukommen.
- 5.4 Sofern die Verantwortung für die Datenverarbeitung beim Auftragnehmer von einer Ärztin oder einem Arzt getragen wird, sind folgende Vorgaben verbindlich:
  - a.) Beim Auftragnehmer eingesetzte Mitarbeiterinnen und Mitarbeiter sind, soweit ihnen im Rahmen ihrer Arbeit personenbezogene Patientendaten zur Kenntnis kommen können, als „berufsmäßig tätige Gehilfen des Arztes“ anzusehen und entsprechend einzusetzen und durch den Auftragnehmer über ihre daraus resultierenden Pflichten zu informieren; sie müssen die Einhaltung dieser Pflichten schriftlich zusichern.
  - b.) Der Auftragnehmer verpflichtet die vorgenannten Mitarbeiterinnen und Mitarbeiter auf die ärztliche Schweigepflicht und dokumentiert diese Verpflichtung schriftlich.
- 5.5 Personal, welches mit besonderen Auftraggeberdaten oder sonst mit Daten in Berührung kommen kann, die dem Arzt-/Patientengeheimnis unterliegen, sind über Ziffer 2.4 hinaus mindestens in einer Anlage 2 – Muster für Verpflichtungserklärung entsprechenden Weise zu verpflichten.
- 5.6 Personal, welches die zum Umgang mit besonderen Auftraggeberdaten berechtigt ist, wird dem Auftraggeber durch den Auftragnehmer namentlich benannt; eine entsprechende Auflistung ist in Anlage 3 - Mitarbeiter beigefügt. Änderungen werden durch schriftliche Mitteilung des Auftragnehmers an den Auftraggeber wirksam. Ausnahmen sind in dringenden Notfällen in Absprache mit dem Systemverantwortlichen des Auftraggebers möglich; sie sind zu protokollieren.

## 6. Fernwartung

Sofern der Auftragnehmer zur vertragsgemäßen Durchführung der Leistungen Fernwartungsmaßnahmen<sup>9</sup> durchführt, findet Anlage 4 - Fernwartung Anwendung.

<sup>8</sup> In Deutschland: besonders geschützte Daten i.S.d. § 3 Abs. 9 BDSG.

<sup>9</sup> In Deutschland gibt hierzu die spezielle Regelung des § 11 Abs. 5 BDSG.

## 7. Telekommunikationsdaten

Sofern der Auftragnehmer zur vertragsgemäßen Durchführung der Leistungen auch dem Fernmeldegeheimnis unterliegende Daten, insbesondere Verkehrs-, Nutzungs- oder Abrechnungsdaten wie z.B. die Nummer eines anrufenden Anschlusses, IP-Adressen, Datum, Uhrzeit und Dauer einer Sprachverbindung und andere Daten, die für die Leistungen unter dem Hauptvertrag notwendig sind (nachfolgend zusammen: „Telekommunikationsdaten“) erhält, erhebt, verarbeitet oder speichert, findet **Anlage 5 - Telekommunikationsdaten** Anwendung.

## 8. Kontrollen

Der Auftraggeber hat sich gemäß Art. 17 Abs. 2 EU Datenschutzrichtlinie<sup>10</sup> vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Auftraggeberdaten durch den Auftragnehmer zu überzeugen. Der Auftraggeber kann die laufende Prüfung durch Stichprobenkontrollen vornehmen und sich von der Einhaltung dieser Vereinbarung überzeugen. Hierzu kann der Auftragnehmer eine aktualisierte **Anlage 1 – Technisch-organisatorische Maßnahmen** sowie Testate von Wirtschaftsprüfern, der hauseigenen Revision oder Auditabteilung oder Auditberichte zur IT-Sicherheit und/oder Datenschutz vorlegen.

Der Auftraggeber hält außer in besonders zu begründenden dringlichen Fällen eine Anmeldefrist von mindestens zehn (10) Arbeitstagen (Montag bis Freitag, ausgenommen örtliche Feiertage) ein. Die Prüfung darf den Geschäftsbetrieb des Auftragnehmers nach Möglichkeit nicht beeinträchtigen. Das Ergebnis der Kontrollen wird durch den Auftraggeber in einem Protokoll dokumentiert.

## 9. Vertragslaufzeit, Vertragsende

Die Dauer dieses Vertrages zur Auftragsdatenverarbeitung entspricht der Laufzeit des Hauptvertrages. Mit Beendigung des Hauptvertrages ist auch dieser Vertrag beendet. Es gelten die Kündigungsregelungen des Hauptvertrages.

Für den Fall fehlender Regelungen zur Vertragslaufzeit gilt dieser Vertrag zur Auftragsdatenverarbeitung auf unbestimmte Zeit abgeschlossen. Beide Parteien können diesen Vertrag mit einer Frist von sechs Monaten zum Ende eines Kalenderjahres schriftlich kündigen.

## 10. Schlussbestimmungen

- 10.1 Der Auftragnehmer wird auch über das Ende des jeweiligen Vertrags hinaus Stillschweigen über die Auftraggeberdaten bewahren.
- 10.2 Mit Ende des Hauptvertrages gibt der Auftragnehmer die Auftraggeberdaten samt Datenträger heraus oder vernichtet sie auf Wunsch nach dem Stand der Technik unwiederbringlich. Der Auftragnehmer ist auch dann zur Vernichtung berechtigt, wenn die Auftraggeberdaten weder geholt werden noch innerhalb von sechs (6) Wochen nach dem Ende des Hauptvertrags Weisung zur

<sup>10</sup> In Deutschland: § 11 Abs. 2 Satz 4 BDSG.

Vernichtung erteilt wird. Ausgenommen sind zwingend aufzubewahrende Daten und Datenträger, für die diese Vereinbarung bis zu deren Vernichtung fort gilt.

- 10.3 Der Auftragnehmer kann für die hierin beschriebenen Maßnahmen einschließlich Prüfungen eine Vergütung verlangen. Im Zweifel gelten seine allgemeinen Stunden- und Tagessätze.
- 10.4 Es gibt keine mündlichen Nebenabreden. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis. Durch E-Mail wird die Schriftform nicht gewahrt. Im Tagesgeschäft kann die Kommunikation auch elektronisch mit Wirkung für und gegen die jeweilige Partei erfolgen, wenn nicht ausdrücklich Schriftform vereinbart wurde. Erkennbar von einer Partei ausgehende elektronische Kommunikation wird dieser zugerechnet.

Die

Anlage 1 – Technisch-organisatorische Maßnahmen

Anlage 2 – Muster für Verpflichtungserklärung

Anlage 3 – Mitarbeiter

Anlage 4 – Fernwartung

Anlage 5 – Telekommunikationsdaten

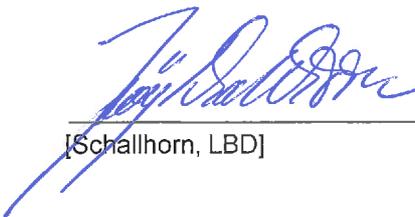
Anlage 6 – Subunternehmer

sind wesentlicher Bestandteile dieser Vereinbarungen.

Der Hauptvertrag bleibt im Übrigen unberührt.

Für den Auftraggeber

Für den Auftragnehmer

  
\_\_\_\_\_  
[Schallhorn, LBD]

  
\_\_\_\_\_  
M. Seifert M. Jansen

Hannover, 06.04.2017

Lübeck, 06.04.2017

## **Anlage 1 zum Vertrag über Auftragsdatenverarbeitung – Technisch-organisatorische Maßnahmen**

Der Auftragnehmer stellt Server bei einem externen Provider seiner Wahl zur Verfügung (derzeit Atos). Im Rahmen des EVB-IT Systemvertrags stellt der Auftragnehmer dem Auftraggeber die Anwendung Drägerware.ZMS/FeuerON, im Folgenden kurz FeuerON genannt, zur Verfügung und führt die gesamte Systemadministration durch. Der Auftraggeber ist Betreiber von FeuerON.

### **1. Zutrittskontrolle**

Der Zutritt zu IT-Systemen wird Unbefugten durch folgende Maßnahmen verwehrt: Am Standort Lübeck und Stuttgart erfolgt eine dienstausweisbasierte Kontrolle beim Geländeeingang. Die Zutrittskontrollregelungen des Subunternehmers Atos sind ebenso wenig Bestandteil dieser TOM ebenso wie Maßnahmen, die in der Verantwortung des Auftragsgebers liegen.

Besucher werden angemeldet und haben nur in Begleitung des Auftragnehmers Zutritt. Besucher oder Externe, die über einen längeren Zeitraum für Dräger tätig sind, erhalten einen Ausweis mit begrenzter Gültigkeit.

Sowohl für den Standort Lübeck als auch die Niederlassung Stuttgart ist ein Wachdienst beauftragt. Der Standort Lübeck ist videoüberwacht.

### **2. Zugangskontrolle**

2.1 An den Dräger-Rechnern erfolgt die Windows Anmeldung über einen persönlichen Account mit Passwort. Passworteigenschaften (Länge, Komplexität, Gültigkeitszeitraum) werden zentral definiert und konfiguriert.

Die Server, auf denen die Anwendung bereitgestellt wird, werden unter LINUX betrieben. Der administrative Zugang ist durch Passwörter gesichert. Gemeinsame Passwörter (z.B. für den Zugriff auf die Datenbank) werden in einem Passwortsafe (Software) verwaltet. Der Server ist nur über **einen** Rechner aus dem Dräger-Netzwerk heraus erreichbar.

Für die administrativen Zugänge haben die Administratoren jeweils personalisierte Benutzerkennungen mit einem persönlichen Passwort, das alle drei Monate geändert werden muss. Für diese Passwörter ist organisatorisch folgendes festgelegt: Länge: muss mindestens 10 Zeichen umfassen und Großbuchstaben, Zahlen und Sonderzeichen enthalten. Die eigentliche Systemadministration erfolgt über einen Sprungserver mittels Secure-Shell (ssh). Auf dem Server ist das SUDO-Konzept umgesetzt.

Die unbefugte Nutzung der Anwendung FeuerON wird durch die Vergabe von benutzerbezogenen Passwörtern verhindert. Die Passworrichtlinie ist durch den Auftraggeber vorgegeben und ist in der Anwendung (Länge, Sonderzeichen ...) umgesetzt. Auf Wunsch des Auftraggebers ist die Anwendung nicht durch zusätzliche Browserzertifikate geschützt.

2.2 Alle Änderungen an Daten werden durch die Anwendung in einer Historie protokolliert. Die Überprüfung der Historie ist Sache des Auftraggebers.

2.3 Systemadministrative Maßnahmen werden vom Auftragnehmer in einem Trackingsystem (derzeit Mantis) dokumentiert.

### 3. Zugriffskontrolle

- 3.1 Die Sicherung der Datenträger oder Dateien gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen, die die einzelnen Anwender aus dem System heraus über die Anwendung erzeugen können, liegt im Verantwortungsbereich des Auftraggebers. Die entsprechenden organisatorischen Maßnahmen sind durch den Auftraggeber zu treffen.
- Im Rahmen seiner administrativen Tätigkeit erstellt der Auftragnehmer Backups der Datenbank und der Anwendung auf einen Backupserver.
  - Im Rahmen der Notfallvorsorge wird ein verschlüsseltes Backup auf einem zusätzlichen externen Backupserver vorgehalten. Dieser Server befindet sich in einem anderen Rechenzentrum (derzeit Hetzner). Die Übertragung der Dateien in dieses Rechenzentrum erfolgt verschlüsselt. Die Verschlüsselung erfolgt derzeit mittels GPG.
- 3.2 Es erfolgt derzeit täglich nachts (zwischen 2:00 und 5:00 Uhr) eine Datensicherung als SQL-Dump der Datenbank über ein Backup-Script. Dieses wird automatisiert über einen cron-job ausgeführt.
- 3.3 Es werden beim Auftragnehmer mindestens die Sicherungen gemäß Sicherungskonzept vorgehalten.

Auf dem Backup-Server werden die folgenden Sicherungen vorgehalten:

7	Tagessicherungen	für die jeweils vergangene Woche
4	Wochensicherungen	für die jeweils vergangenen vier Wochen
12	Monatssicherungen	für die jeweils vergangenen zwölf Monate
X	Jahressicherungen	für alle vergangenen Jahre

- 3.4 Die Vergabe der Zugriffsrechte beim Auftragnehmer erfolgt nach dem Need-to-Know Prinzip. Im Rahmen der Systemadministration hat ein eingeschränkter Personenkreis Zugriff auf die Anwendung.

Die Berechtigungsvergabe innerhalb der Anwendung für die Zugriffe der Anwender liegt in der Verantwortung des Auftraggebers. Dazu sind folgende Maßnahmen vorgesehen:

differenzierte Zugriffsberechtigung auf

- Datensätze
- Datenfelder

Weiter bestehen innerhalb der Anwendung differenzierte Einstellungen für die Verarbeitungsmöglichkeiten

- Lesen
- Ändern
- Löschen

Die Einstellung der Rechteverwaltung innerhalb der Anwendung erfolgt durch den Auftraggeber.

Die Überprüfung der Zugriffsberechtigung erfolgt automatisch durch die Anwendung.

Die Protokollierung der Systemnutzung erfolgt durch Log- Dateien auf dem Server, die im Rahmen der Serverwartung regelmäßig durch den Auftragnehmer gelöscht werden.

#### **4. Weitergabekontrolle**

- 4.1 Im Rahmen der Serveradministration versendet der Auftragnehmer keine Daten.
- 4.2 Die Privatnutzung von Hard- und Software ist beim Auftragnehmer gemäß Konzernrichtlinie nicht erlaubt.
- 4.3 Magnetische Datenträger werden bei Aussonderung durch Überschreiben oder auch durch physische Zerstörung datenschutzgerecht gelöscht.

Optische Datenträger (Papier) werden über einen Reißwolf datenschutzgerecht vernichtet.

- 4.4 Es erfolgt kein Transport von Datenträgern.
- 4.5 Folgende Dienste werden zur Weitergabe personenbezogener Daten genutzt:

- e-Mail: nur auf Aufforderung des Auftraggebers, www (Tracker) und SFTP.

Folgende Sicherheitsmaßnahmen sind implementiert:

- Firewall SSL, https

- 4.6 Im Rahmen der Auftragsdatenverarbeitung werden vom Auftragnehmer lediglich verschlüsselte Datensicherungen übertragen.

#### **5. Eingabekontrolle**

Die Änderungen der Anwendungsstruktur bzw. des Systems durch Administratoren werden über den Tracker beauftragt und protokolliert.

Ob und von wem Daten im Anwendungssystem eingegeben, verändert oder entfernt worden sind, kann durch Protokollierung eingegebener Daten und Verarbeitungsprotokolle nachträglich überprüft und festgestellt werden.

#### **6. Auftragskontrolle**

- 6.1 Es existieren Verträge für folgende Formen der Auftragsdatenverarbeitung:

- Auftragsdatenverarbeitungsvertrag zum EVB-IT Systemvertrag

- 6.2 Die Verarbeitung personenbezogener Daten im Auftrag wird nur entsprechend den Weisungen des Auftraggebers durchgeführt. Diese erfolgen durch schriftliche Anweisungen über E-Mail oder über das eingesetzte Trackingsystem.
- 6.3 Änderungen und Erweiterungen am Anwendungssystem können vom Auftraggeber über das eingesetzte Trackingsystem nachvollzogen werden. Darüber hinaus werden bei der Freigabe der einzelnen Programmversionen bzw. Patches vom Auftragnehmer jeweils Releasehistorien erstellt, die dem Auftraggeber vorab zur Verfügung gestellt werden.
- 6.4 Der Auftragnehmer hat jederzeit die Möglichkeit, sich über die Fehlersituation im Anwendungssystem über das eingesetzte Trackingsystem zu informieren. Bei wesentlichen Fehlern erfolgt zusätzlich eine Information des Auftraggebers per E-Mail.

6.5 Die Administration der Server erfolgt ausschließlich über eine SecureShell-Verbindung. Auf den eingesetzten Servern ist das SUDO-Konzept eingerichtet, so dass keine Administratorkennung auf dem System vorhanden ist.

6.6 Eine Fernwartung findet beim Anwender nicht statt.

## 7. Verfügbarkeitskontrolle

7.1 Folgende Maßnahmen zur Sicherung der Daten gegen zufällige Zerstörung oder Verlust sind implementiert:

- Tägliches Backup der gesamten Datenbank (siehe auch Ziff. 3.2 / 3.3).
- Zusätzlicher Backupserver.

7.2 Es wird nach dem oben beschriebenen Sicherungskonzept gesichert.

7.3 Es gibt Sicherungen, die in anderen Brandabschnitten gelagert sind.

7.4 Sicherungsprotokolle werden regelmäßig auf Auffälligkeiten durch den DrägerService geprüft.

7.5 Vor Versionswechsel werden regelmäßig Tests zur Rückspeicherung der Datensicherungen durchgeführt. Zusätzlich werden die Daten beim Einrichten / Umzug eines Servers aus der Datensicherung wiederhergestellt.

7.6 Es existiert folgende Planung für den Katastrophenfall: Aufsetzen eines neuen Servers und Rückspielen der letzten Datensicherung.

## 8. Trennungsgebot

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt voneinander verarbeitet.

Dazu sind folgende Maßnahmen implementiert:

- Softwareseitiger Ausschluss (Mandantentrennung).
- Trennung von Test- und Echtanwendung.
- Trennung von Test- und Echtdateien (Testdateien werden auf Anforderung des Auftraggebers mit den Echtdateien überschrieben).



Anlage 2 zum Vertrag über die Auftragsdatenverarbeitung

**Anlage 2 – Muster für Verpflichtungserklärung**

**Verpflichtung auf das Datengeheimnis**

Sehr geehrte(r) Frau/Herr ,

Ziel des Datenschutzes ist der Schutz natürlicher Personen (Mitarbeiter, Kunden, Lieferanten und andere Partner) vor Missbrauch ihrer personenbezogenen Daten<sup>1</sup>. Im Rahmen Ihrer Tätigkeit für Dräger haben Sie Zugang zu personenbezogenen Daten und gilt für Sie das Datengeheimnis nach den gesetzlichen Vorschriften über den Datenschutz. Sie sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung erhoben, verarbeitet oder genutzt werden. Jeder Missbrauch, vor allem jede unbefugte Erhebung, Verarbeitung, Nutzung oder Weitergabe dieser Daten, ist unzulässig.

Nach den gesetzlichen Vorschriften über den Datenschutz sind Sie verpflichtet, das Datengeheimnis zu wahren. Diese Verpflichtung besteht auch über das Ende Ihrer Tätigkeit für unser Unternehmen hinaus fort.

Wir weisen Sie darauf hin, dass Verstöße gegen das Datengeheimnis mit Freiheits- oder Geldstrafe geahndet werden können. Auch Schadensersatzansprüche können bei einer unbefugten Erhebung, Verarbeitung oder Nutzung von Daten bestehen. Abschriften der hierin erwähnten und für Sie einschlägigen gesetzlichen Vorschriften über den Datenschutz sind beigefügt.

Ihre sich ggf. aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Anweisungen ergebende allgemeine Geheimhaltungsverpflichtung wird durch diese Erklärung nicht berührt.

Bitte unterzeichnen Sie die Erklärung auf der nachfolgenden Seite, auf der Sie den Erhalt und die Kenntnisnahme dieser Informationen bestätigen und übermitteln diese an Ihren Vorgesetzten.

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift : Vorname, Name

<sup>1</sup> \* Personenbezogene Daten sind Angaben zu einer bestimmten oder bestimmaren natürlichen Person, die elektronisch in Datenverarbeitungsanlagen oder in nicht automatisierten Dateien gespeichert sind, z. B. Name, Geburtsdatum, Körpergröße, gesundheitliche Verfassung, Einkommen, Familienstand oder auch Verbindungsdaten in der Telekommunikation.

**Bestätigung**

**Über die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes wurde ich unterrichtet. Die sich daraus ergebenden Verhaltensweisen wurden mir mitgeteilt. Meine Verpflichtung auf das Datengeheimnis habe ich hiermit zur Kenntnis genommen und werde ich dieses wahren.**

---

Ort, Datum

---

Unterschrift der Mitarbeiterin  
bzw. des Mitarbeiters

Anlage 3 zum Vertrag über die Auftragsdatenverarbeitung

**Anlage 3 – Mitarbeiter**

Artur Brinkmann  
Friedwalt Brinkmann  
Susanne Haß  
Erik Jünger  
Heike Kessler  
Dirk-Kirsten Ruprecht

## Anlage 4 zum Vertrag über die Auftragsdatenverarbeitung

### Anlage 4 – Fernwartung

1. Der Auftragnehmer wird bei der Durchführung von Fernwartungsmaßnahmen nicht auf Daten zugreifen, die nicht Gegenstand der vereinbarten Fernwartung sind. Der Auftragnehmer wird den mit der Fernwartung betrauten Personen nur die zur Durchführung der konkreten Aufgaben nötigen Berechtigungen erteilen. Der Auftraggeber übermittelt hierzu Vorgaben an den Auftragnehmer oder richtet entsprechende Benutzerkonten ein.
2. Der Auftragnehmer wird bei der Durchführung der Fernwartung die Weisungen und Vorgaben des Auftraggebers beachten. Es werden keine Maßnahmen durchgeführt, die nicht zwischen den Parteien vereinbart sind. Insbesondere wird der Auftragnehmer ohne Einwilligung des Auftraggebers (a) keine Einsicht in Auftraggeberdaten nehmen oder Kopien von Auftraggeberdaten anfertigen, deren Kenntnis zur Erledigung der Fernwartung nicht erforderlich ist und (b) keine eigenen Test- und Wartungsprogramme dauerhaft auf dem fernzuwartenden System ablegen. Eine Speicherung von Auftraggeberdaten auf Rechnern außerhalb des Bereichs des Auftraggebers erfolgt nur auf Weisung des Auftraggebers.
3. Die die Fernwartungsmaßnahme durchführende Person hat die von ihr ergriffenen Maßnahmen zu dokumentieren, ohne dabei personenbezogene Daten festzuhalten. Die Dokumentation wird dem Auftraggeber im Anschluss an jeden Fernwartungsvorgang übersandt und nach Durchsicht von einer oder einem der Systemverantwortlichen des Auftraggebers gegengezeichnet und abgelegt.
4. Die Freigabe des zu wartenden Systems zur Fernwartung erfolgt in jedem Einzelfall durch einen Mitarbeiter des Auftraggebers. Dazu wird ein neu vergebenes Zugangskennwort mittels E-Mail [zuverlässig verschlüsselt] übermittelt. Falls die Person auf Seiten des Auftragnehmers den Kooperationspartner auf Seiten des Auftraggebers zuverlässig an der Stimme erkennen kann, ist ersatzweise auch die telefonische Mitteilung des Kennworts (nach Anruf des Auftraggebers beim Auftragnehmer) statthaft.
5. Es ist nicht statthaft und mittels technischer Vorgaben auszuschließen, dass mit einem System des Auftraggebers ohne Verwendung sicherer Verschlüsselungsverfahren über ein Netzwerk oder eine Telefonleitung kommuniziert wird.
6. Die eigentliche Fernwartung verläuft nicht direkt zwischen einem Rechner des Auftragnehmers und dem zu wartenden System; vielmehr ist zwischen diese beiden Geräte ein dritter Rechner zwischengeschaltet, der der Zugriffskontrolle und Protokollierung dient. Für die Kommunikation zwischen den drei beteiligten Systemen wird – unter Einsatz von Verschlüsselung – ein Fernsteuerverfahren benutzt; die näheren Einzelheiten sind in den technisch-organisatorischen Maßnahmen festgehalten.
7. Während des gesamten Fernwartungsvorgangs muss eine Mitarbeiterin oder ein Mitarbeiter des Auftraggebers beim System anwesend und für den Auftragnehmer telefonisch erreichbar sein. Alle Eingaben, die bei der Fernwartung seitens des Auftragnehmers erfolgen, sowie die daraus resultierenden Ausgaben des Systems müssen während der Fernwartung vom Personal des Auftraggebers beobachtet werden und sind beim Auftragnehmer in geeigneter Weise auf Datenträger zu protokollieren.
8. Wird die Verbindung mehr als 20 min nicht genutzt, wird sie durch den Auftraggeber unterbrochen und bei Bedarf nach dem oben beschriebenen Verfahren erneut hergestellt.
9. Vor Zugriff auf personenbezogene Daten holt der Auftragnehmer in jedem Einzelfall die

## Anlage 4 zum Vertrag über die Auftragsdatenverarbeitung

Zustimmung eines Systemverantwortlichen des Auftraggebers ein. Die Übertragung personenbezogener Daten zum Auftragnehmer per Dateitransfer, auf Datenträger oder mittels download, erfolgt nur auf Weisung des Auftraggebers.

10. Bei der Wartung oder Fernwartung übertragene oder auf beweglichem Datenträger festgehaltene Daten werden nicht an Dritte weitergegeben und zuverlässig gelöscht, sobald sie nicht mehr zur Erfüllung der vertraglich vereinbarten Wartungsarbeiten benötigt werden.
11. Unmittelbar nach Beendigung jeder Fernwartung wird das zu diesem Zweck vergebene Zugangskennwort vom Personal des Auftraggebers durch ein neues ersetzt.
12. Der Auftragnehmer gewährleistet, die Fernwartung ausschließlich in dem Land des Auftraggebers, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum durchzuführen, oder mit dem Auftraggeber Maßnahmen zu vereinbaren, mit deren Hilfe ein solche Tätigkeit auch aus dem Nicht-EU-Ausland zulässig ist, insbesondere den Abschluss von Verträgen mit den jeweils aktuellen Standardvertragsklauseln.
13. Die Fernwartung erfolgt wenn irgend möglich in Testumgebungen; der Zugriff auf das Produktivsystem wird nur gewählt, wenn ein Wartungsziel anders nicht erreicht werden kann.
14. Beide Parteien dürfen eine Fernwartungsmaßnahme bei Unklarheiten über deren rechtmäßigen Verlauf sofort abbrechen.

## Anlage 5 – Telekommunikationsdaten

1. Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer Telekommunikationsdaten im erforderlichen Umfang nutzen, verarbeiten und/oder an Dritte übermitteln darf, um
  - a.) geschuldete Leistungen zu erbringen,
  - b.) Verwaltung, Abrechnung und Buchhaltung über die Leistungen durchzuführen,
  - c.) Telekommunikationseinrichtungen des Auftraggebers zu warten,
  - d.) die technische Qualität der Leistungen zu überwachen,
  - e.) Missbrauch von Leistungen aufzudecken und vorzubeugenund im Übrigen immer dann, wenn vom Auftraggeber beauftragt, regulatorisch vorgeschrieben oder durch Gerichtsentscheidung oder aufgrund einer Maßnahme einer Behörde erforderlich.
2. Der Auftraggeber holt alle erforderlichen Einwilligungen und Erlaubnisse (einschließlich Betroffener wie z.B. Personal des Auftraggebers) für die hier beschriebene Nutzung, Verarbeitung und Übermittlung von Telekommunikationsdaten ein hat und hält diese für die Dauer des Hauptvertrags aufrecht und holt diese auch zukünftig rechtzeitig ein.
3. Falls nicht anders vereinbart, darf der Auftragnehmer Telekommunikationsdaten für sechs (6) Monate ab deren Erfassung speichern. Danach werden die Telekommunikationsdaten gelöscht, wenn nicht der Auftraggeber eine andere Weisung erteilt.

Anlage 6 zum Vertrag über Auftragsdatenverarbeitung

**Anlage 6 – Subunternehmer**

Für die Bereitstellung oder Anmietung eines Servers:

**Atos IT Solutions and Services GmbH**  
Otto-Hahn-Ring 6  
D-81739 München