Vertrag für die Auftragsverarbeitung (Art. 28 DS-GVO)

zwischen

Hessisches Ministerium des Innern und für Sport

Friedrich-Ebert-Allee 12

65185 Wiesbaden

(„Auftraggeber")

und

Dräger Safety AG & Co. KG aA

Revalstraße 1

23560 Lübeck

(„Auftragsverarbeiter")

Der Gegenstand dieses Vertrages ist die datenschutzgerechte Erledigung der im Überlassungsvertrag vom 03./10.07.1995 und im Änderungsvertrag vom 11./28.11.2007 zwischen dem Auftragnehmer und dem Auftraggeber („Hauptvertrag") vereinbarten Leistungen (Bereitstellung und Betrieb der Drägerware.ZMS/FLORIX Hessen). Hierzu werden nachfolgende Vereinbarungen getroffen:

Im Brand- und Katastrophenschutz des Landes Hessen tätige Behörden, Dienststellen und Einrichtungen des Landes, der Landkreise und der Gemeinden sowie die Werkfeuerwehren nach § 14 Hessisches Brand- und Katastrophenschutzgesetz können eine Lizenz zur Nutzung der Drägerware.ZMS/FLORIX Hessen erwerben. Ferner können mit besonderer Genehmigung des Hessischen Ministeriums des Innern und für Sport weitere im Brand- und Katastrophenschutz mitwirkende Organisationen und Personen Lizenzen für die Drägerware.ZMS/FLORIX Hessen erwerben.

Das Land Hessen, vertreten durch das Hessische Ministerium des Innern und für Sport (HMdIS) ist „Auftraggeber" und die Dräger Safety AG & Co. KG aA „Auftragsverarbeiter".

Jeder Lizenznehmerin und jeder Lizenznehmer (nachfolgend: Lizenznehmer genannt), die/der mit Dräger Safety AG & Co. KG aA einen Lizenzvertrag abschließt, ist datenschutzrechtlich für die von ihr/ihm in Drägerware.ZMS/FLORIX Hessen eingestellten Daten „Verantwortlicher" nach Art. 4 Nr. 7 der Richtlinie 95/46/EG vom 27. April 2016 (Datenschutz-Grundverordnung – DS-GVO). Dräger Safety AG & Co. KG aA übernimmt gegenüber allen Lizenznehmern die Aufgaben des „Auftragsverarbeiter" nach Art. 4 Nr. 8 DS-GVO.

1. Anwendungsbereich

1.1. Der Auftragsverarbeiter ist gemäß Hauptvertrag vom Auftraggeber mit der Erbringung von Leistungen für den Bereich

- Gesamtbereich Datenverarbeitung,

- Wartung von IT-Infrastruktur,
- Fernwartung über Telekommunikationsleitungen

beauftragt. Dabei ist nicht auszuschließen, dass der Auftragsverarbeiter im Zuge der vertragsgemäßen Durchführung der Leistungen die Möglichkeit des Zugriffs auf personenbezogene Daten, die vom Auftraggeber bzw. von den Lizenznehmern als Verantwortliche dieser Daten oder aus deren Sphäre stammen (nachfolgend: Daten), hat und diese verarbeiten werden.

1.2. Dieser Vertrag über die Auftragsverarbeitung enthält die dabei zu beachtenden allgemeinen Anforderungen und gilt für alle Datenverarbeitungsaufträge des Auftraggebers sowie der Lizenznehmer an den Auftragsverarbeiter. Er ergänzt und konkretisiert die Regelungen zum Datenschutz im Hauptvertrag. Im Fall von Widersprüchen zu dem Hauptvertrag gehen die Regelungen dieser Vereinbarung vor.

2. Auftragsinhalt

2.1. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- Daten von Feuerwehrangehörigen und ggf. weiteren Mitgliedern aus den Feuerwehrvereinen,
- Einsatzdaten,
- Benutzerdaten.

Die Übersicht der personenbezogenen Daten ist in der **Anlage 1 – Felder im Modul Personal** dargestellt. Die Daten in nicht als „auch nach § 55 HBKG abgedecktes Datenfelder" enthaltenen Feldern sind von der datenbesitzenden Person freiwillig und selbst, im Regelfall schriftlich, für die Datenverarbeitung zur Verfügung gestellt. Sie können nach § 3 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetz zur Erfüllung der Aufgaben im Brand- und Katastrophenschutz erhoben werden.

2.2. Von der Verarbeitung betroffen sind folgende Personengruppen:

- Feuerwehrangehörige und ggf. weitere Mitglieder aus den Feuerwehrvereinen,
- Personen, die im Zusammenhang mit Einsätzen, Ausbildungs- und sonstigen Dienstveranstaltungen stehen und im Berichtswesen dokumentiert werden,
- Personen, denen persönliche Ausrüstungsgegenstände oder Bekleidungsteile zugordnet sind, und in der Geräteverwaltung dokumentiert werden,
- Personen, die als Ansprechpartner für die Anforderung von Sondereinsatzmittel und –einheiten in der Datenbank für Sondereinsatzmittel und-einheiten hinterlegt sind.

2.3. Weitere Arten der Datenverarbeitung:

- Das Verfahren dient der zentralen Verwaltung von Daten der im Brand- und Katastrophenschutz des Landes Hessen tätigen Behörden, Dienststellen und Einrichtungen des Landes, der Landkreise und der Gemeinden sowie der Werkfeuerwehren und mit besonderer Genehmigung des Hessischen Ministeriums des Innern und für Sport weiteren im Brand- und Katastrophenschutz mitwirkenden Organisationen und Personen.
- Bei den Feuerwehren bzw. den Kommunen werden Daten erfasst, ausgewertet und abgefragt. Im Rahmen der Aufsicht können die Landkreise personenbezogene Daten zur Wahrnehmung ihrer Aufsichtsfunktion einsehen. Ansonsten können die Landkreise, die Regierungspräsidien und der Auftraggeber im Rahmen der Aufsichtstätigkeit, der

Informationsgewinnung zur Brandschutzförderung und der Gefahrenabwehrplanung zur Erstellung von Statistiken auf keine personenbezogenen Daten zurückgreifen.

- Lediglich die Erreichbarkeiten (Adresse, Tel-Nr., E-Mail-Adresse) von Führungskräften und Jugendfeuerwehrwarten ist über alle Ebenen sichtbar.
- Ein weiteres Verfahren stellt die Anmeldung zu Lehrgängen und Seminaren an der Hessischen Landesfeuerwehrschule (HLFS) und auf Landkreisebene dar. Bei der Anmeldung werden persönliche Daten von den Feuerwehren über die Landkreise an die HLFS bzw. den Landkreis als Ausbildungsstätte gesandt. Das Ergebnis der Teilnahme an den Lehrgängen und Seminaren (bestanden/teilgenommen) wird von der HLFS oder den Landkreisen über das Verfahren in die persönlichen Daten des Teilnehmers in die Personalverwaltung der Feuerwehr bzw. der Behörde oder Dienststelle übertragen. Der Eintrag erfolgt über einen Statuswechsel: der Statuswechsel erfolgt im Regelfall von „angemeldet" über „einberufen" zu „bestanden" oder „teilgenommen". Weiter werden Daten von Teilnehmern an Lehrgängen und Seminaren an der HLFS über eine Schnittstelle an eine Software zur Schulbetriebssteuerung und -verwaltung gegeben.
  In der Datenbank für Sondereinsatzmittel und –einheiten werden u.U. zuständige Personen mit Namen und Erreichbarkeit dokumentiert. Dies gilt insbesondere für Fachberater und zuständige Ansprechpartner bei privaten Unternehmen. Diese Personen selbst haben keinen Zugang zu ZMS Florix Hessen.

3. Pflichten des Auftragsverarbeiters

3.1. Der Auftragsverarbeiter beachtet bei der Verarbeitung von Daten des Auftraggebers und der Lizenznehmer die Datenschutz-Grundverordnung (DS-GVO), das Hessische Datenschutz- und Informationsfreiheitsgesetz (HDSIG), das Hessische Brand- und Katastrophenschutzgesetz (HBKG) sowie weitere geltenden Rechtsvorschriften zum Datenschutz in der jeweils gültigen Fassung, soweit diese für Leistungen des Auftragsverarbeiters gelten, insbesondere Art. 28 DS-GVO. Dies gilt nur, soweit nicht gesetzlich zwingend der Vorrang eines bestimmten Datenschutzgesetzes angeordnet ist. Der Auftragsverarbeiter hat die innerbetriebliche Organisation so zu gestalten, dass sie den gesetzlichen Anforderungen des Datenschutzes gerecht wird.

3.2. Der Auftragsverarbeiter verarbeitet Daten nur im Rahmen des Auftrags und entsprechend den schriftlichen Weisungen des Auftraggebers. Der Auftraggeber und jeder Lizenznehmer bleiben als speichernde und verantwortliche Stelle der „Herr der Daten".

3.3. Inhaltliche Änderungen der Daten sind nur mit Einwilligung des Auftraggebers durchzuführen. Eine Verwendung von Daten in anonymisierter Form für statistische Zwecke oder zur Qualitätsüberwachung der Leistungen des Auftragsverarbeiters ist ausdrücklich gestattet.

3.4. Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach schriftlicher Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar oder mittelbar über den Lizenznehmer an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.5. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Vorschriften über den Datenschutz verstößt, weist der Auftragsverarbeiter den Auftraggeber unverzüglich in Textform darauf hin. Der Auftragsverarbeiter unterrichtet den Auftraggeber und die Lizenznehmer auf dem gleichen Weg binnen 72 Stunden bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder bei anderen wesentlichen Unregelmäßigkeiten bei der Verarbeitung der Daten.

Ebenso wird der Auftragsverarbeiter Verstöße gegen Weisungen des Auftraggebers unaufgefordert anzeigen. Der Auftragsverarbeiter unterrichtet den Auftraggeber außerdem unverzüglich, wenn eine Aufsichtsbehörde ihm gegenüber tätig wird und das Vorgehen die Auftragsverarbeitung aus dieser Vereinbarung betrifft.

3.6. Der Auftragsverarbeiter ist verpflichtet, bei der Verarbeitung von Daten ausschließlich Personal einzusetzen, das zur Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurde. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3.7. Der Auftragsverarbeiter gewährleistet die Einhaltung seiner gesetzlichen Verpflichtungen gemäß Art. 28 bis 33 DS-GVO wie folgt:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- Dieser Datenschutzbeauftragte ist unter der Email **dataprivacy@draeger.com** und der Telefonnummer **+49 451 882 6030** zu erreichen.

3.8. Der Auftragsverarbeiter wird nach Beendigung der Vertragsbeziehung alle Daten an den Auftraggeber bzw. die Lizenznehmer zurückgeben oder, nach Absprache mit dem Auftraggeber bzw. den Lizenznehmern, löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Lizenznehmer bzw. der Auftraggeber.

3.9. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben. Der Auftragsverarbeiter stellt auf schriftliche Anfrage des Auftraggebers die erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung.

3.10. Der Auftragsverarbeiter meldet dem Auftraggeber und den Lizenznehmern nach Art. 33 Abs. 2 DS-GVO unverzüglich die Verletzung von personenbezogenen Daten mit

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, der Kategorie,
- der ungefähren Anzahl der betroffenen Personen, der ungefähren Anzahl von Datensätzen und der betroffenen Kategorien,
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Person oder Anlaufstelle, von der weitere Informationen erhältlich sind,
- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- Beschreibung der bereits ergriffenen Maßnahmen zur Behebung der Datenschutzverletzung und ggf. zur Abmilderung ihrer möglichen nachteiligen Auswirkungen,
- Vorschlag weiterer einzuleitenden Maßnahmen.

3.11. Darüber hinaus unterstützt er den Auftraggeber und die Lizenznehmer

- bei der Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung

durch Sicherheitslücken berücksichtigen (Sicherheit der Verarbeitung) und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

- bei der Meldepflicht gegenüber dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit als zuständige Aufsichtsbehörde nach Art. 33 Abs. 1 DS-GVO und der Benachrichtigung der betroffenen Personen nach Art. 34 DS-GVO bei einer Verletzung des Schutzes personenbezogener Daten durch unverzügliche Zurverfügungstellung sämtlicher relevanten Informationen,
- bei der Erstellung der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO,
- bei den vorherigen Konsultationen mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit als zuständige Aufsichtsbehörde nach Art. 36 DS-GVO,
- mit geeigneten technischen und organisatorischen Maßnahmen bei der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen nach Kap. III DS-GVO.

Für Unterstützungsleistungen darüberhinaus kann der Auftragsverarbeiter eine Vergütung beanspruchen.

3.12. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

3.13. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

3.14. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

3.15. Auf Verlangen des Auftraggebers stellt der Auftragsverarbeiter alle Informationen zum Nachweis der Einhaltung der aus diesem Vertrag sich ergebenen Pflichten zur Verfügung und ermöglicht und unterstützt den Auftraggeber oder einen von ihm beauftragten Prüfer bei der Überprüfung.

4. Subunternehmer

4.1. Leistungen von Subunternehmen bzw. Unterauftragsdatenverarbeitern sind Leistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist gleichwohl verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

4.2. Der Auftraggeber muss nach Art. 28 Abs. 2 S. 1 DS-GVO durch vorherige schriftliche Genehmigung der Hinzuziehung von Subunternehmern bzw. Unterauftragsdatenverarbeiter zustimmen.

4.3. Werden Subunternehmer bzw. Unterauftragsdatenverarbeiter eingesetzt, gewährleistet der Auftragsverarbeiter die vertragliche Absicherung des Datenschutzes auf dem durch diese Vereinbarung festgelegten Niveau und die Ergreifung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO durch den Unterauftragsverarbeiter.

4.4. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter nach DS-GVO die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 5.1 Abs. 1 Satz 2 eingesetzt werden sollen.

5. Pflichten des Auftraggebers und der Lizenznehmer

5.1. Der Auftraggeber beurteilt die Zulässigkeit der Verarbeitung von Daten gemäß Art. 6 Abs. 1 DS-GVO in Verbindung mit dem Hessische Datenschutz- und Informationsfreiheitsgesetz und dem Hessischen Brand- und Katastrophenschutzgesetz durch den Auftragsverarbeiter im Rahmen des Auftrags gemäß den Regelungen der DS-GVO und anderer anzuwendender Vorschriften über den Datenschutz. Der Auftraggeber sowie die Lizenznehmer stellen sicher, dass die Daten zweifelsfrei aus dem jeweiligen Herrschaftsbereich stammen und ordnungsgemäß erhoben wurden bzw. werden.

5.2. Der Auftraggeber sowie die Lizenznehmer werden den Auftragsverarbeiter unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten unterrichten, insbesondere bei der Prüfung der Ergebnisse der Auftragsdatenverarbeitung.

5.3. Der Auftraggeber und die Lizenznehmer als „Verantwortliche" wahren die Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO und den Schutz deren persönlicher Daten. Sie sind informationspflichtig nach Art. 13 DS-GVO gegenüber den Personen, deren personenbezogene Daten sie erheben. Sie sind für die unverzügliche und möglichst binnen 72 Stunden zu erfolgende Meldung an den Hessischen Beauftragten für Datenschutz und Informationsfreiheit als zuständige Aufsichtsbehörde nach Art. 33 Abs. 1 DS-GVO mit folgenden Informationen nach Art. 33 Abs. 3 DS-GVO

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, der Kategorie,
- der ungefähren Anzahl der betroffenen Personen, der ungefähren Anzahl von Datensätzen und der betroffenen Kategorien,
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Person oder Anlaufstelle, von der weitere Informationen erhältlich sind,
- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- Beschreibung der bereits ergriffenen Maßnahmen zur Behebung der Datenschutzverletzung und ggf. zur Abmilderung ihrer möglichen nachteiligen Auswirkungen und
- Vorschlag weiterer einzuleitenden Maßnahmen

zuständig und haben die betroffenen Personen, deren Daten von einer Verletzung des Schutzes betroffenen sind, nach Art. 34 DS-GVO zu benachrichtigen.

5.4. Der Auftraggeber erteilt dem Auftragsverarbeiter unverzüglich die zur Beantwortung von Auskunftsverlangen der Datenschutzaufsichtsbehörde (Art. 58 DS-GVO) nötigen Weisungen.

5.5. Soweit der Auftraggeber oder ein Lizenznehmer die Daten selbst als Auftragsverarbeiter für einen Dritten verarbeitet und die Tätigkeit des Auftragsverarbeiters daher eine Unterauftragsdatenverarbeitung darstellt, stellen der Auftraggeber bzw. der betreffende Lizenznehmer sicher, dass der Dritte "Herr der Daten" und Verantwortlicher im Sinne der DS-GVO bleibt und die ihm nach der DS-GVO zustehenden Rechte hat. Der Auftragsverarbeiter wird in diesen Fällen nur beauftragt, wenn zuvor die Genehmigung des Dritten eingeholt wurde. Der Auftraggeber bzw. der betreffende Lizenznehmer stellen außerdem sicher, dass dem Auftragsverarbeiter die gleichen Datenschutzpflichten auferlegt werden, wie dem Auftraggeber bzw. dem betreffenden Lizenznehmer selbst aus dem Auftragsverarbeitungsvertrag mit dem Dritten auferlegt sind. Der Auftraggeber bzw. der betreffende Lizenznehmer werden bei mehreren Auftraggebern vertraglich Vorsorge tragen, dass solche Anfragen vom Auftraggeber koordiniert und gesammelt und vom Auftraggeber bzw. von dem betreffenden Lizenznehmer stellvertretend für die Dritten bearbeitet werden. Dies gilt nicht bei konkreten erheblichen Beanstandungen der Dritten, für die der Auftragsverarbeiter verantwortlich ist.

5.6. Allgemeine Weisungen des Auftraggebers für den Umgang mit Daten bedürfen der Textform. Mündliche Weisungen des Auftraggebers im Einzelfall dürfen nur durch hierzu autorisierte Personen erfolgen.

6. Weitere Vertragszwecke

6.1. Der Auftragsverarbeiter hat das Recht, die von dieser Vereinbarung umfassten personenbezogenen Daten zu anonymisieren und vorher die für die Anonymisierung erforderlichen Verarbeitungsschritte durchzuführen.

6.2. Der Auftragsverarbeiter ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Fehlerbehebung in dem Produkt, in dem die Daten gespeichert sind, zu verarbeiten, sowie anonymisierte Daten aus dem Produkt abzuziehen.

6.3. Der Auftragsverarbeiter ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Entwicklung neuer oder Weiterentwicklung bestehender Produkte in einer angemessen gesicherten Umgebung zu verarbeiten. Der Auftragsverarbeiter berücksichtigt auch in diesem Verarbeitungsprozess, dass vom Kunden gelöschte oder zur Löschung angewiesene Daten nicht mehr verarbeitet werden.

7. Kontrollen

7.1. Der Auftraggeber hat sich gemäß Art. 28 Abs. 1 DS-GVO vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten durch den Auftragsverarbeiter zu überzeugen.

Soweit die Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Der Auftraggeber kann die laufende Prüfung durch Stichprobenkontrollen vornehmen und sich von der Einhaltung dieser Vereinbarung überzeugen. Hierzu kann der Auftragsverarbeiter eine aktualisierte **Anlage 2 – Technisch Organisatorische Maßnahmen** sowie Testate von Wirtschaftsprüfern, der hauseigenen Revision oder Auditabteilung oder Auditberichte zur IT-Sicherheit und/oder Datenschutz vorlegen.

7.2. 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 Auftragsverarbeiters nach Möglichkeit nicht beeinträchtigen. Das Ergebnis der Kontrollen wird durch den Auftraggeber in einem Protokoll dokumentiert.

8. Haftung

8.1. Auftraggeber und Auftragsverarbeiter haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

8.2. Der Auftraggeber und der Lizenznehmer stellen den Auftragsverarbeiter von Ansprüchen Dritter frei, einschließlich der Kosten der angemessenen Rechtsverteidigung, die in Zusammenhang mit der Auftragsdatenverarbeitung erhoben werden. Im Hauptvertrag vereinbarte Haftungsbeschränkungen gelten insofern 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 Auftragsverarbeiter hat oder der Auftragsverarbeiter eine ihn aus Art. 82 Abs. 2 Satz 2 DS-GVO treffende Pflicht schuldhaft verletzt.

9. Vertragslaufzeit, Vertragsende

9.1. 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.

9.2. Ein außerordentliches Kündigungsrecht besteht bei schwerwiegendem Datenrechtsverstoß.

10. Schlussbestimmungen

10.1. Sollten die Daten des Auftraggebers oder eines Lizenznehmers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber und den jeweiligen Lizenznehmer unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Betroffenen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber und den Lizenznehmern als „Verantwortliche" im Sinne der DS-GVO liegen.

10.2. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Vertrages zur Auftragsverarbeitung unwirksam sein, so berührt dies die Wirksamkeit der in der Anlage 2 enthaltenen technisch organisatorische Maßnahmen nicht.

10.3. Der Auftragsverarbeiter wird auch über das Ende des jeweiligen Vertrags hinaus Stillschweigen über die Daten bewahren.

10.4. Mit Ende des Hauptvertrages gibt der Auftragsverarbeiter die Daten samt Datenträger heraus oder vernichtet sie auf Wunsch nach dem Stand der Technik unwiederbringlich. Der Auftragsverarbeiter ist auch dann zur Vernichtung berechtigt, wenn die Daten weder geholt werden noch innerhalb von sechs (6) Wochen nach dem Ende des Hauptvertrags Weisung zur Vernichtung erteilt wird. Ausgenommen sind zwingend aufzubewahrende Daten und Datenträger, für die diese Vereinbarung bis zu deren Vernichtung fort gilt.

10.5. Der Auftragsverarbeiter kann für die hierin beschriebenen Maßnahmen einschließlich Prüfungen eine Vergütung verlangen. Im Zweifel gelten seine allgemeinen Stunden- und Tagessätze.

10.6. 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.

10.7. Die **Anlage 2 – Technisch Organisatorische Maßnahmen Dräger** ist Bestandteil dieser Vereinbarung. Die dort beschriebenen Maßnahmen hat der Auftragsverarbeiter bei gegebenen Anlass, mindestens aber jährlich einer Überprüfung, Bewertung und Evaluierung der Wirksamkeit zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO durchzuführen. Das Ergebnis ist dem Auftraggeber mitzuteilen.

11. Beitritt zu diesem Vertrag

Zur Regelung der datenschutzrechtlichen Belange können im Brand- und Katastrophenschutz des Landes Hessen tätige Behörden, Dienststellen und Einrichtungen des Landes, der Landkreise und der Gemeinden, die Werkfeuerwehren nach § 14 Hessisches Brand- und Katastrophenschutzgesetz sowie mit besonderer Genehmigung des Hessischen Ministeriums des Innern und für Sport weitere, im Brand- und Katastrophenschutz mitwirkende Organisationen und Personentätige Organisationen diesem Vertrag durch einseitige Erklärung beitreten. Hierzu schließen diese Organisationen vorab jeweils einen eigenen Hauptvertrag (Lizenzvereinbarung) mit dem Auftragsverarbeiter ab.

Der Hauptvertrag bleibt im Übrigen unberührt.

Für den Auftraggeber	**Für den Auftragsverarbeiter**
Wiesbaden, 04.10.2018	Lübeck 6.11.18
Ort, Datum	Ort, Datum

Dräger

Technisch Organisatorische Maßnahmen

bei

Vertrieb & Service

Deutschland

Dräger Medical Deutschland GmbH

Dräger TGM GmbH

Dräger Medical Ansy GmbH

Dräger Safety AG & Co. KGaA

im weiteren „Dräger"

Inhaltsangabe

1 Zutrittskontrolle

Zutrittskontrolle fasst jene Maßnahmen zusammen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Bei Dräger erfolgt eine Zutrittskontrolle für den Zutritt zum Betriebsgelände bzw. Gebäude und Niederlassungen über

- Berechtigungsausweis
- Zutritt zum Firmengelände durch Haupt-/ Nebentore, die mit Kartenlesegeräten ausgestattet und durch Pförtner überwacht sind.
- Türschlösser mit Zugangscode
- Zutritt zum Funktionsbereich durch Kartenlesegerät mit reduziertem Berechtigtenkreis gesichert.
- Alarmanlage
- Gebäudeüberwachung

2 Zugangskontrolle

Zugangskontrolle fasst jene Maßnahmen zusammen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Bei Dräger wird die unbefugte Nutzung von IT-Systemen verhindert durch

- User-ID und Passwort
- Bildschirmsperre mit Passwortaktivierung
- Fernwartung nur über ein Portalsystem mit eigenen Zugriffscodes und einem dedizierten Berechtigungskonzept.
- Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort. Das Passwort ist wie folgt aufgebaut und wird in den folgenden zeitlichen Abständen gewechselt:
  - Mindestzeichenlänge von 8 Zeichen
  - Mindestens ein Kleinbuchstabe
  - Mindestens ein numerisches Zeichen
  - Mindestens ein Sonderzeichen
  - Das Passwort wird alle 90 Tage gewechselt
- Funktionelle Zuordnung der Datenendgeräte zu Nutzern
- Ein dediziertes Rollen-/ Rechtekonzept für jedes Gerät

3 Zugriffskontrolle

Zugriffskontrolle steht für jene Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Jeder Mitarbeiter wird zu Beginn seines Arbeitsverhältnisses auf das Datengeheimnis verpflichtet und erhält eine Einführung zum Umgang mit personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnissen der Kunden.
Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

Für die relevanten IT-Systeme, mit denen insbesondere personenbezogene Daten verarbeitet werden, bestehen Berechtigungskonzepte, mit denen der Zugriff auf darin gespeicherte personenbezogene Daten aus technischer Sicht nur denjenigen Anwendern möglich gemacht wird, die dazu auch die erforderliche Rolle/ die damit verbundene Berechtigung besitzen.
Zur Bearbeitung von Supportfällen benötigte Daten werden auf dem Kundensystem verarbeitet. Eine dauerhafte Speicherung von Kundendaten auf den Systemen von Dräger findet nicht statt. Ist es in besonderen Fällen notwendig Daten auf lokalen Rechnern bei Dräger zu analysieren (z.B.: Eskalation an die Produktentwicklung) so werden verschlüsselte Laufwerke eingesetzt. Darüber hinaus werden außer Betrieb genommene Speichermedien einem kontrollierten und dokumentierten Zerstörungsprozess zugeführt.
Evtl. angefertigte Ausdrucke werden zur Entsorgung in verschlossene Datenschutzcontainer geworfen, die in einem datenschutztechnisch geprüften Prozess von einem spezialisierten Dienstleister entsorgt werden, mit dem ein gültiger Auftragsdatenverarbeitungsvertrag besteht.

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 der Anwendung auf einen Backupserver. Im Rahmen der Notfallvorsorge wird zusätzlich ein externes Backup vorgehalten.

Datensicherungen und Recovery

Die Datenträger, auf denen der Auftragnehmer die extern zu lagernden Sicherungen aufbewahrt, sind verschlüsselt und werden in einem vom Server getrennten Feuerschutzbereich gelagert.

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.

Im Nachgang werden das Sicherungsergebenis der Datenbank, die Konfigurationsdateien, die Server-Zertifikate, das Backupscript und die Log-Dateien der Sicherung sowie die aktuelle Anwendung in eine Datei gepackt, die anschließend verschlüsselt und auf einen Backup- Server übertragen wird (Tagessicherungsdatei).

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

Da sich der Backup-Server im gleichen Rechenzentrum wie der Anwendungsserver befindet, wird zusätzlich zur Archivierung die jeweils aktuelle Tagessicherungsdatei auch auf ein Sicherungsmedium übertragen.

In Desaster-Recovery-Fall: kompletter Systemausfall, der ein Neuaufsetzen erforderlich macht, wird jeweils auf die neueste Datensicherung zurückgegriffen.

4 Weitergabekontrolle

Die Weitergabekontrolle fasst jene Maßnahmen zusammen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Auf den Rechnern und im Netz von Dräger werden die folgenden Sicherheitsmaßnahmen verwendet:

- Virenschutz
- Firewalls
- Netzsegmentierung
- VPN (Virtual Private Networks) für möglichen Fernzugriff
- Content Filter / Proxys
- IPS /IDS (Intrusion Detection /Prevention Systems) an den Internet Outbreaks
- Verschlüsselung von E-Mails

5 Eingabekontrolle

Eingabekontrolle steht für jene Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Das Fernwartungssystem von Dräger speichert automatisch die Verbindungsdetails: Vorname, Nachname, Telefonnummer, E-Mail-Adresse, Region, Portalzugang, Organisation, Login, Logout, Verbindungsbeginn/ -ende, UserID, genutztes Protokoll, Datenmenge ein- und ausgehend.
Die in der Sitzung möglicherweise stattgefundenen Zugriffe auf personenbezogene Daten beim Kunden (eine Änderung oder Löschung von personenbezogenen Daten im Kundensystem ist prinzipiell nicht Bestandteil der Fernwartung) werden manuell dokumentiert.
Sollte eine Änderung oder Löschung von personenbezogenen Daten in einem besonderen Fall nötig sein, so geschieht das nur nach Freigabe und Anweisung des Auftraggebers und wird dementsprechend protokolliert.

Die Daten verändernden Zugriffe auf personenbezogene Daten durch die einzelnen Benutzer des Systems werden durch die Anwendung in einer Historie für jeden Datensatz protokolliert. Dabei werden neben dem Benutzer auch der Zeitpunkt sowie die Art der Bearbeitung (vorheriger Wert/nachheriger Wert) festgehalten. Berechtigte Benutzer können diese Historie einsehen. Die Historieneinträge werden durch das System nach einen einstellbaren Zeitraum gelöscht. Der Löschzeitraum wir durch den Auftraggeber vorgegeben und in Form eines täglichen Löschlaufes ausgeführt.

6 Auftragskontrolle

Unter Auftragskontrolle sind jene Maßnahmen zusammengefasst, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Sofern ein anderes Unternehmen als „Subunternehmer" Dienstleistungen für Dräger erbringt und in diesem Zusammenhang auch personenbezogene Daten erhoben, verarbeitet und genutzt werden, trägt Dräger dafür Sorge, dass der „Subunternehmer" sorgfältig ausgewählt wird und die Auswahl sich insbesondere an dem Aspekt des Schutzes personenbezogener Daten orientiert. Die Beauftragung von „Subunternehmern" bedarf aber in jedem Fall der Zustimmung des Auftraggebers. Die Beauftragung von Dienstleistern erfolgt auf der Basis der bei Dräger gültigen Standards und sieht eine Information an den Bereich Datenschutz sowie eine Kontrolle des Auftragnehmers im Hinblick auf die von ihm getroffenen technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit vor. Dräger verpflichtet seine Auftragnehmer, die gesetzlichen Vorgaben zum Schutz personenbezogener Daten zu treffen und insbesondere auch auf Anfrage nachzuweisen, dass die Mitarbeiter, die im Rahmen der Erbringung von Leistungen für Dräger tätig werden, auf das Datengeheimnis verpflichtet wurden. Dräger nimmt von seinem Recht Gebrauch, schriftliche Weisungen bezüglich Art, Zweck und Umfang der Verarbeitung personenbezogener Daten an den Auftragnehmer erteilen und die Einhaltung der Vorgaben durch Kontrollen sicherstellen.

Die relevanten Auftragnehmer sind:

- Dienstleister zum Betrieb und Management der Client Rechner sowie der darauf genutzten Software
- Dienstleister Betrieb und Management des Netzes und der Netzzugänge
- Dienstleister zur Entsorgung von Papierbasierten Dokumenten und elektronischen Speichermeiden

7 Verfügbarkeitskontrolle und Notfallplanung

Verfügbarkeitskontrolle und Notfallplanung beschreibt jene Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Bei Dräger werden Daten des Auftraggebers nicht solchermaßen lokal verarbeitet, dass Kundenprozesse davon direkt abhängig wären. Ein Ausfallen der Systeme bei Dräger hätte schlimmstenfalls nur zur Folge, dass die anhängige Wartung verschoben werden müsste.
Das Fernwartungssystem wird im Rechenzentrum eines Dienstleisters von Dräger betrieben. Mittels SLAs wird sichergestellt, dass die Systeme ausfallsicher betrieben werden.

8 Trennungskontrolle

Die Trennungskontrolle beinhaltet all jene Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Durch die folgenden Maßnahmen ist die Sicherung der getrennten Speicherung, Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken gewährleistet:

- Die zur Verarbeitung von Kundendaten verwendeten Systeme sind mandantenfähig bzw. Kundenspezifisch.
- Test- und Produktivsysteme sind funktional getrennt.

9 Fernwartung

Fernwartung umfasst diejenigen Maßnahmen, die gewährleisten, dass der räumlich getrennte Zugriff auf IT-Systeme zu Wartungs- und Reparaturzwecken geschützt vor dem Zugriff unberechtigter erfolgen kann. Dies erfolgt nur in den Fällen, wenn dies mit den Kunden vertraglich vereinbart und die technischen Voraussetzung dafür getroffen wurden.

9.1 Prinzipiell Zugangsart

wird das Kundensystem über eine Site-to-Site, bzw. SSL-VPN-Verbindung zu dedizierten Systemen des Auftraggebers erreicht. Dort wo 24/7 Supportverträge bestehen, ist ein 24/7 Zugriff auf die Einwahlknoten Bedingung. Die Fernwartung wird fast ausschließlich auf Serversystemen durchgeführt, der Endanwender der Kunden arbeitet an abgesetzten Arbeitsstationen, auf die nur im absoluten Ausnahmefall in Abstimmung mit dem Personal vor Ort zugegriffen wird.

9.2 Verbindungsaufbau

Schematisch wird der Verbindungsaufbau wie folgt realisiert:
Fernwartungsrechner im Dräger-internen Netz -> Dräger ServiceConnect RDC Access Server (über SSH) -> zu wartendes System des Auftraggebers (über App.Protocol)

Der Verbindungsaufbau lässt sich detaillierter in zwei voneinander getrennten Kommunikationsverbindungen beschreiben:

- Fernwartungsrechner über das ServiceConnect RDC Portalsystem zum Access Server
- Access Server zum System des Auftraggebers

Fernwartungsrechner über das ServiceConnect RDC Portalsystem zum Access Server
Der Fernwartungsrechner im Dräger-Intranet verbindet sich zum ServiceConnect RDC Portal. Nach einer Authentifizierung kann der Anwender nur auf die ihm zugewiesenen Geräte des Auftraggebers zugreifen und einen Device-Connect (Remoteverbindung) aufrufen. Bei diesem Device-Connect leitet der ServiceConnect RDC Portal-Server den HTTPS-Stream zum Access Server. Der ServiceConnect RDC Access-Server lädt auf dem Fernwartungsrechner ein Connect-Applet (upload). Das Connect-Applet stellt eine Point-2-Point SSL verschlüsselte SSH Tunnel dar. D.h. es gibt einen SSH-Tunnel zwischen Fernwartungsrechner und ServiceConnect RDC Access Server. Das Connect-Applet startet das lokal vorhandene bzw. vom Access Server hochgeladene Applikationsprotokoll zur Fernwartung auf dem Fernwartungsrechner. Der Client des Applikationsprotokolls auf dem Fernwartungsrechner führt den zugehörigen, spezifischen Applikationsprotokoll-Dialog mit dem Connect Applet. Das Connect Applet leitet ohne Kenntnis der Dateninhalte diesen Applikationsprotokoll-Dialog als Datenpaket zum Access-Server.

Access Server zum System des Auftraggebers

Der Access-Server terminiert den Point-2-Point SSL verschlüsselten SSH Tunnel und entpackt die Datenpakete des Connect-Applet. Der Access-Server baut eine separate, zweite Verbindung zum Auftraggeber-Device (über einen physikalisch getrennten MUX Server in einer weiteren DMZ) auf. In diese zweiten Verbindung werden die entpackten Datenpakete des Connect-Applets erneut verpackt und die Rückantworten werden dem Connect Applet in der ersten Verbindung mitgeteilt. Es gibt keine direkte Point-2-Point Verbindung vom Dräger Intranet zum Auftraggeber IP-Netz (oder Device). Die Verbindungen zwischen dem Fernwartungsrechner und der Access Server DMZ sind auswärts initiiert, verschlüsselt und nur über Port 26 (Connect Applet) bzw. 443 (HTTPS redirect) freigeschaltet. Die zweite Kommunikationsverbindung zwischen Access Server und Device verwendet die zugrundeliegenden Ports und IP-Protokoll (tcp/udp). Hierbei verwendet der Access Server die Kommunikationsverbindungen IPSec für Router, SSLVPN für VPN, IP over Intranet, etc.

9.3 Sicherheitsmaßnahmen

Ferner ist sichergestellt, dass

- Die Remote-Verwaltungssoftware sich bei Verbindungsabbruch beendet
- Der Auftraggeber jederzeit die Fernwartung abbrechen kann
- Eine Protokollierung des Zugriffs stattfindet

10 Physische Sicherheit

Im Rahmen der physischen Sicherheit gewährleisten wir, dass Dräger-eigene Gebäude und Flächen in Raumklassen eingeteilt werden. Diese Einteilung erfolgt abhängig von der Nutzung und dem damit verbundenen Schutzbedarf. Der Schutzbedarf orientiert sich an den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und den damit verbundenen Risiken. Abhängig von der Raumklasse setzen wir unterschiedliche physische Maßnahmen um. Dazu zählen insbesondere:

- Zutrittssicherung: Die Maßnahme umfasst bauliche Maßnahmen, um nicht Berechtigte am Zutritt für sie gesperrte Bereiche zu hindern.
  Dazu zählen bei Dräger u.a. Umfriedungen, Vereinzelungsanlagen sowie baulicher Einbruchsschutz an Türen und Fenstern.
- Zutrittskontrolle: Die Maßnahme umfasst die Überprüfung des rechtmäßigen Zutritts zu Flächen und Gebäuden.
  Dazu zählen bei Dräger Videoüberwachung, Streckenüberwachungen, Wachgänge, Ausweiskontrolle, Schlüsselmanagement.
- Branderkennung und Brandbekämpfung: Die Maßnahme umfasst bauliche Vorsorge zur Minimierung des Brandrisikos sowie Technologien um frühzeitig Brände zu identifizieren und diese wirkungsvoll zu unterbinden.
  Dazu gehören bei Dräger Brandabschnitte, Feuer- und Rauchmelder sowie Feuerlöschsysteme, die auf das Zielobjekt angepasst sind.
- Verfügbarkeitskontrolle: Diese Maßnahme umfasst Absicherungen gegen Ausfall von Infrastrukturelementen.
  Dazu gehören bei Dräger redundante Auslegungen kritischer Infrastrukturen mit Prozessen, die einen möglichst reibungslosen Übergang von der einen auf die andere Infrastruktur gewährleisten.
- Ununterbrochene Stromversorgung: Die Maßnahme umfasst die Absicherungsmethoden gegen Stromausfall.
  Dazu gehören bei Dräger neben der redundant ausgelegten Stromversorgung auch Notstromaggregate und eine Batterie-Pufferung, um die Systeme im Notfall weiter betreiben oder kontrolliert herunterfahren zu können.

- Elementarschutz: Diese Maßnahme umfasst Absicherungen gegen Elementarschäden wie Blitze, Hochwasser und Sturm.
  Dazu gehören bei Dräger Blitzableiter, Sicherungen der Fenster und Schotten an den Toren.
- Klimatisierung: Die Maßnahme umfasst die Sicherstellung der notwendigen Betriebstemperatur der Infrastrukturelemente.
  Dazu gehören bei Dräger in der Regel redundant ausgelegte Klimaanlagen, aber auch Entfeuchtungsanlagen und Heizungen.
- Prozess zur Außerbetriebnahme von Speichergeräten: Diese Maßnahme beschreibt, wie Speichermedien behandelt werden, die nicht mehr benötigt werden.
  Dazu gehört bei Dräger entweder das Überschreiben mit zufälligen oder unkenntlichen Daten oder die physische Zerstörung, i.d.R. durch Schreddern.

Entsprechend den Anforderungen an die eigene physische Sicherheit achten wir darauf, dass unsere Lieferanten und Dienstleister diese oder mindestens gleichwertige Maßnahmen umsetzen.

11 Das ISMS bei Dräger

Die Informationssicherheit bei Dräger ist die Verantwortung und Verpflichtung aller. Egal, ob Mitarbeiter, Geschäftspartner oder sonstige Beteiligte mit der Information in Berührung kommen oder diese verarbeiten. Geordnet und gesteuert wird dies aus dem Informations-Sicherheits-Management-System, kurz ISMS, bei Dräger. Dieses ISMS besteht aus den folgenden Kernbereichen:

- Strategie & Prinzipien
- Organisation
- Prozesse
- Kommunikation & Training
- Monitoring & Reporting

Gemeinsam mit der Unternehmensführung und den beteiligten Fachbereichen werden die **Strategie & Prinzipen** im Rahmen der Informationssicherheit für Dräger festgelegt.

Die **Organisation** des ISMS und seine Kontrolle erfolgt aus dem Information Security Council (ISC). Die Kernmitglieder des ISC sind der Konzerndatenschutzbeauftragte, der Koordinator des Dräger-Risikokomitees und der CIO. Das ISC entscheidet über interne Richtlinien und Prozesse. Darüber hinaus bewertet das ISC gemeldete Risiken zur Informationssicherheit und legt Maßnahmen zur Mitigation fest. In übergreifenden Fragen wird das ISC um weitere Fachbereiche erweitert.

Zu den wesentlichen **Prozessen**, mit denen das ISMS bei Dräger umgesetzt wird, zählen eine global gültige Richtlinie, ein Handbuch zur Informationssicherheit sowie verschiedene verbundene Prozesse und Handlungsanweisungen.

Im Rahmen der **Kommunikation** etablieren wir Mechanismen, um alle Mitarbeiter und Geschäftspartner zu erreichen und Bewusstsein für Informationssicherheit zu schaffen. Dazu gehören auch **Trainings** zum Informationsschutz, die alle unsere Mitarbeiter durchlaufen müssen. Damit stellen wir sicher, dass die Kernelemente unseres ISMS und Kontaktmöglichkeiten innerhalb unserer Organisation bekannt sind. Das kontinuierliche Streben gilt hier dem Ziel, dass alle Mitarbeiter, die Unternehmensführung und Dräger verbundene Dritte sich ihrer Verantwortung und den Risiken im Umgang mit Informationen bewusst sind und die etablierte Informationssicherheitsstrategie nach Kräften unterstützen.

Monitoring und **Reporting** liefern einen wesentlichen Beitrag zum ISMS, indem sie für die notwendige Transparenz sorgen, damit wir die Informationssicherheit weiterhin kontinuierlich verbessern können.

Personenbezogene Daten in ZMS Florix Hessen - Anlage 1 zum AVV

Felder im Modul Personal		**Legende:**	
		Zugriffsrechte	
		Mussfeld zur programmtechn. Eingabe einer Person	
		nach § 55 HBKG abgedecktes Datenfeld	
Reiter	**Reiter**	**Feldbezeichnung**	**Erläuterungen**
Person	Neue Person	Personal-Nr.	
		Nachname	auch nach § 55 HBKG abgedecktes Datenfeld
		Vorname	auch nach § 55 HBKG abgedecktes Datenfeld
		Geschlecht	
		Geburtsdatum	auch nach § 55 HBKG abgedecktes Datenfeld
		Organisation	auch nach § 55 HBKG abgedecktes Datenfeld
		Art/Abteilung	auch nach § 55 HBKG abgedecktes Datenfeld
Person	**Persönliche Daten**	Titel/Akad. Grad	
		Spind-Nr.	
		Anrede	
		Brieftitel	
		Familienstand	
		Anzahl Kinder	
		Auch Mitglied in	
		Staatsang.	kann beamtenrechtliche Bedeutung haben
		Organisationswechsel	
		Blutgruppe	
		Straße	
		Hausnummer	
		Nation	
		PLZ	
		Ort	
		Ortsteil	
		Telefon privat	
		Telefon dienstlich	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Telefax privat	
		Telefax dienstlich	
		Mobil privat	
		Mobil dienstlich	
		E-Mail privat	
		E-Mail dienstlich	
		Einstellungsdatum	
		Verstorben am	
		Dienstgrad	
		Person nicht in Personalstatistik berücksichtigen	kein Textfeld, Datenverarbeitungshinweis
		Dienststellung	
		Für Einsätze der gesamten Stadt/Gemeinde freigeben	kein Textfeld, Datenverarbeitungshinweis
		Einsatzfahrer	
		Person hat der Weitergabe der Daten widersprochen	kein Textfeld, Datenverarbeitungshinweis
		Atemschutzüberwachung nach FwDV7	kein Textfeld, Datenverarbeitungshinweis
		Barcode Atemschutz	
Person	**Erreichbarkeiten**	Art	
		Nummer	
		Erreichbarkeit 1	
		Erreichbarkeit 2	
Person	**Familienereignisse**	Ereignis	
		Am	
		Ort	
		Bemerkung 1	
		Bemerkung 2	
Person	**Bild**		
Person	**Biografie**		
Person	**Zusatz Biografie**	Bezeichnung	
		Von	
		Bis	
		Ort	
		Ablauf 1	
		Ablauf 2	
Person	**Geburtsdaten**	Geburtsort	
		Geburtsname	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
Person	**Beruf**	Berufsausbildung/Beruf	
		Land	
		Von	
		Bis	
		Ausbildungsort	
		Besondere Fähigkeiten 1	
		Besondere Fähigkeiten 2	
Feuerwehr	**Art/Abteilung**	Art/Abteilung	Mussfeld, siehe oben
		Von	
		Bis	
		Ort	
		Bundesland	
		Austrittsgrund	
		In Statistik nicht auswerten	kein Textfeld, Datenverarbeitungshinweis
		Nähere Informationen 1	
		Nähere Informationen 2	
Feuerwehr	**Dienstgrad**	Dienstgrad/Beförderung	
		Abk. Dienstgrad	
		Von	
		Bis	
		Ort	
		Beförderungsgrund 1	
		Beförderungsgrund 2	
Feuerwehr	**Ausbildungen**	Lehrgangsbezeichnung	
		Von	
		Bis	
		Lehrgangsort	
		Begründung	für Lehrgangsanmeldungsverfahren
		Begründung/Rückst.	für Lehrgangsanmeldungsverfahren
		Anmerkungen	für Lehrgangsanmeldungsverfahren
		Veranstalter	für Lehrgangsanmeldungsverfahren
		Status	für Lehrgangsanmeldungsverfahren
		Anzahl Rückst.	für Lehrgangsanmeldungsverfahren
		Anmeldedatum	für Lehrgangsanmeldungsverfahren
Feuerwehr	**Zutrittsberechtigungen**	Zutrittsberechtigungen	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Schlüssel erhalten	
		Schlüssel abgegeben	
		Schlüsselnummer	
		Grund 1	
		Grund 2	
Feuerwehr	Ausweise	Bezeichnung	
		Ausweisnummer	
		Von	
		Bis	
		Versanddatum	
		Rückerhalt	
		Vernichtung	
		Inhalt 1	
		Inhalt 2	
Feuerwehr	Ehrungen	Bezeichnung	wichtig für zu beantragende Ehrungen (aufsteig. Reihenfolge:
		Am	Bronze, Silber, Gold) sowie beim Beantragungsverfahren
		Beantragt am	wichtig beim Beantragungsverfahren
		Status	wichtig beim Beantragungsverfahren
		Ort	wichtig beim Beantragungsverfahren
		Verleiher/Grund 1	
		Verleiher/Grund 2	
Feuerwehr	Abzeichen/Nachweise	Bezeichnung	
		Am	
		Ort	
		Inhalt 1	
		Inhalt 2	
Feuerwehr	Wehrdienst		
Feuerwehr	Stellenplan	Haushaltsstelle	
		Stellennummer	
		Stellenwert	
		Stellenwert pers.	
		Stunden laut SP	
		Stunden pers.	
Einsatzdienst	Zug/Gruppe	Zug/Gruppe	
		Von	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Bis	
		Ort	
		Funktion 1	
		Funktion 2	
Einsatzdienst	**Dienststellung**	Dienststellung/Fkt.	
		Von	
		Bis	
		Ende der Wahlperiode	
		Ort	
		Funktion 1	
		Funktion 2	
		Auswertung der Erreichbarkeiten	
Einsatzdienst	**Tauglichkeiten**	Bezeichnung	
		Von	
		Gültig bis	
		Ort	
		Auflagen Stichwort	
		Info 1	
		Info 2	
		Tätigkeit	
		Dauer (min)	
		Info Atemschutz	
Einsatzdienst	**Fahrerlaubnis**	Fahrerlaubnis-Klasse	
		Von	
		Bis	
		Ausstellungsbehörde	
		Erweiterungen/Auflagen 1	
		Erweiterungen/Auflagen 2	
Einsatzdienst	**Rufkombinationen**		
Einsatzdienst	TETRA-Pager		
Einsatzdienst	**Persönliche Ausrüstung**		
Einsatzdienst	**Impfungen**	Impfung	
		Impfschutz ab	
		Impfschutz bis	
		Auffrischung Impfschutz am	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Arztgespräch am	
		Anmerkung	
Andere Dienste	Überörtliche Tätigkeit	Überörtliche Tätigkeit	
		Überörtliche Tätigkeit kurz	
		Von	
		Bis	
		Ort	
		Tätigkeit 1	
		Tätigkeit 2	
Andere Dienste	KatS-Tätigkeiten	KatS-Einheit	
		KatS-Einheit kurz	
		Von	
		Bis	
		Ort	
		Tätigkeit 1	
		Tätigkeit 2	
Andere Dienste	Funktionen	Funktion	
		Von	
		Bis	
		Ort	
		Aufgaben/Sachgebiet 1	
		Aufgaben/Sachgebiet 2	
Andere Dienste	Abwesenheit	Stichwort	
		Von Datum	gehört zu Erreichbarkeiten nach § 55 HBKG
		Bis Datum	gehört zu Erreichbarkeiten nach § 55 HBKG
		Telefon	gehört zu Erreichbarkeiten nach § 55 HBKG
		Ort	gehört zu Erreichbarkeiten nach § 55 HBKG
		Grund 1	
		Grund 2	
Andere Dienste	Beurlaubung	Beurlaubung von	gehört zu Erreichbarkeiten nach § 55 HBKG
		Von	gehört zu Erreichbarkeiten nach § 55 HBKG
		Bis	gehört zu Erreichbarkeiten nach § 55 HBKG
		Grund	
Andere Dienste	Verfügbarkeit	Wochentag	gehört zu Erreichbarkeiten nach § 55 HBKG
		Von Uhrzeit 1	gehört zu Erreichbarkeiten nach § 55 HBKG

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Bis Uhrzeit 1	gehört zu Erreichbarkeiten nach § 55 HBKG
		Von Uhrzeit 2	gehört zu Erreichbarkeiten nach § 55 HBKG
		Bis Uhrzeit 2	gehört zu Erreichbarkeiten nach § 55 HBKG
		Schicht	
		Grund 1	
		Grund 2	
Adressen	Angehörige	Art	
		Priorität	
		Vorname	
		Nachname	
		Titel	
		Anrede	
		Brieftitel	
		Straße	
		Hausnummer	
		Nation	
		PLZ	
		Ort	
		Telefon privat	
		Telefon dienstlich	
		Telefax	
		Mobiltelefon	
		eMail	
		Sonstiges	
Adressen	Arbeitgeber	Arbeitgeber	
		Abteilung	
		Titel	
		Anrede	
		Brieftitel	
		Ansprechpartner	
		Straße	
		Hausnummer	
		Nation	
		PLZ	
		Ort	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		Funktion dort	
		Telefon privat	
		Telefon Arbeitgeber	
		Telefax	
		Mobiltelefon	
		eMail	
		Sonstiges	
Finanzen	**Bankverbindung**	**Bank**	
		Ort	
		Bankleitzahl	
		BIC	
		Inhaber	
		Kontonummer	
		IBAN	
		Mandatsreferenz	
		Mandatsreferenz erteilt	
		Lastschriftart	
		Zusatzfeld	
		Beiträge/Spenden	
		Kürzel	
		Auszahlung	
		Kürzel	
		Abrechnungsschlüssel Gebührensatz	
	Beiträge	Jahresbeitrag	
		Beitragstyp	
		Beitragsart	
		Zahlungsweise	
		Mandatsreferenz	
		Gültig ab	
		Erste Fälligkeit	
		Nächste Zahlung	
		Kostenstelle	
		Zeitung	
		Januar	
		Februar	

Reiter	Reiter	Feldbezeichnung	Erläuterungen
		März	
		April	
		Mai	
		Juni	
		Juli	
		August	
		September	
		Oktober	
		November	
		Dezember	
Sonstige	**Dokumente**	Bezeichnung	
		Datei	
	Katalog	Eintrag	
	Fremdsprachen	Sprache	
		Verstehen	
		Lesen	
		Sprechen	
		Schreiben	
		Anmerkung	
		Muttersprache	
Historie		Änderungshistorie	