Dräger Smart Rescue System
Nutzungsbedingungen

Version 2.0

Stand 04.12.2020

1 Vertragsparteien

Der von Ihnen geschlossene Vertrag über die Nutzung des Dräger Smart Rescue System, z.B. nach Ablauf der kostenlosen Testphase, **(der "Vertrag")** wird zwischen Ihnen **(“Auftraggeber“ oder „Sie“)** und Dräger Safety AG & Co. KGaA **("Auftragnehmer", „Dräger“ oder „wir“)** abgeschlossen. Wenn Sie ein Unternehmen oder sonstige juristische Person oder Körperschaft öffentlichen Rechts vertreten („Organisation“), erklären und garantieren Sie, dass Sie berechtigt sind, dieser Vereinbarung im Namen Ihrer Organisation zuzustimmen.

2 Leistungsumfang

Der Ihnen zur Verfügung stehende Leistungsumfang ergibt sich aus dem von Ihnen bei Vertragsschluss verwendeten Bestellformular oder dem von uns an Sie gerichteten Angebot.

3 Leistungsbeschreibung

Das Dräger Smart Rescue System (DSRS) ist ein digitales Einsatzinformationssystem für Behörden mit öffentlichen Sicherheitsaufgaben.

Im Folgenden werden die relevanten Bestandteile des DSRS und der damit einhergehende Leistungsumfang näher beschrieben.

3.1 Serviceinfrastruktur zum Betrieb des Dräger Smart Rescue System

Unter Serviceinfrastruktur sind alle Komponenten zum Betrieb der Online-Version des DSRS, der Anbindung der Offline-Clients, das Datenverwaltungsbackend, die Mandantenverwaltung sowie die DSRS-seitigen Schnittstellen zum Zugriff auf Leitstellenschnittstellen zu verstehen. Der Auftragnehmer stellt diese Serviceinfrastruktur, die zum Einsatz des DSRS notwendig ist, vollumfänglich zur Nutzung zur Verfügung und betreibt diese.

3.2 Mandantenverwaltung

Die Mandantenverwaltung stellt Funktionalitäten zur Verwaltung des DSRS zur Verfügung. Hier wird beispielsweise festgelegt, wer in welchem Umfang auf die Anwendung und Daten zugreifen darf. Je nach Mandantentyp, also Datennutzer oder Gebäudedatenbereitsteller, werden unterschiedliche Funktionen bereitgestellt. In der Mandantenverwaltung werden unter anderem die Benutzerkonten verwaltet. Dies beinhaltet zum Beispiel:

- Benutzerkonten anlegen
- Benutzerkonten löschen
- Benutzerkonten ändern

Weiterhin können Art und Umfang der Nutzung der Anwendungen in Teilen gesteuert werden.

3.3 Gebäudeverwaltung

In der Gebäudeverwaltung werden die Nutzdaten der Anwendung verwaltet, also die Daten zu Gebäuden, die im Einsatzfall an die Endgeräte der Rettungskräfte übermittelt werden. In der Gebäudeverwaltung können Daten zu Gebäuden angelegt, geändert und gelöscht werden. Jeder Gebäudeinformationenbereitsteller hat dabei nur Zugriff auf die von ihm angelegten Daten. Ein Zugriff auf die Daten anderer Datenbereitstellungsmandanten ist somit nicht möglich.

Die Funktionalität umfasst die Verwaltung von Gebäuden, die anhand ihrer Adressdaten mittels Geocoding eindeutig identifizierbar sind. Alternativ können fiktive Adressen oder solche, die dem dahinter liegenden Kartendienst nicht bekannt sind, direkt über Geokoordinaten hinzugefügt werden. Zu jedem dieser Gebäude können Metadaten erfasst und verwaltet werden, wie zum Beispiel die Anzahl der Stockwerke, die Anzahl Wohnungen, die Energieversorgung, feuerwehrtechnische Einrichtungen oder Kontaktdaten von Ansprechpartnern der Hausverwaltung. Weiterhin werden hier

Informationen wie Lagepläne, Grundrisse und Ansichten der Gebäude abgelegt und mit zusätzlichen Informationen angereichert.

Daten können sowohl vollständig manuell erstellt werden, als auch teilautomatisiert per Excel nach einem vorgegebenen Schema importiert werden. Die Teilautomatisierung bezieht sich dabei nur auf textgebundene Informationen.

Die Bereitstellung der Nutzdaten obliegt nicht dem Auftragnehmer. Abhängig von der konkreten Vereinbarung unterstützt der Auftraggeber bei der Datenbeschaffung. Unter der Maßgabe, dass die Datenbereitsteller jeweils die mit der Nutzung der Plattform einhergehenden Bedingungen akzeptieren, wird der Auftragnehmer mit den Datenbereitstellern Verträge abschließen, die diesen den Zugriff auf die Plattform ermöglichen. Für die Qualität der Daten kann der Auftragnehmer naturgemäß keine Verantwortung übernehmen.

3.4 Umgebungsplanverwaltung

Nicht alle für die Feuerwehr relevanten Informationen sind einem definierten Gebäude zuzuordnen. So gibt es insbesondere im Fall von durch Feuerwehr oder andere Behörden bereitgestellte Daten Dokumente, welche einer definierten Fläche, beschreibbar durch Koordinatenpunkte, zuzuordnen sind und somit eine Vielzahl von in der Fläche enthaltene Objekte abdecken. Ein gängiges Beispiel hierfür sind Hydrantenpläne.

Die Umgebungsplanverwaltung bietet die Möglichkeit, diese Dokumente in das DSRS einzuspielen und durch Angabe der Eck-Koordinatenpunkte einem rechteckigen Flächenbereich zuzuordnen. Sobald ein Einsatz in diesem Bereich stattfindet, werden die Flächenplandokumente ergänzend zu den objektbezogenen Dokumenten im DSRS dargestellt. Flächenpläne können PDF-Dokumente oder Bilddateien im Format PNG oder JPG < 5 MB sein.

3.5 Offline-Client

Der Offline-Client ist die offlinefähige Version der Einsatzanwendung und damit die Anwendung, die im Einsatzfall Daten zu einem Gebäude auf Tablets oder Laptops der Einsatzleitung anzeigt.
Der Offline-Client wird regelmäßig synchronisiert und ist nach der Synchronisation ohne Internetzugang während eines Einsatzes nutzbar.

Der Offline-Client stellt die folgenden Informationen zu Gebäuden zur Verfügung:

- Digitaler Alarmzettel
- Textgebundene Gebäudeinformationen
- Ansichten
- Lagepläne
- Grundrisse

Beim digitalen Alarmzettel handelt es sich um die Darstellung der heute in der Alarmdepeche enthaltenen Informationen, also insbesondere Einsatzadresse, Einsatznummer, Anfahrt sowie weitere alarmierte Einheiten. Dank dem DSRS sind diese Informationen nicht nur papiergebunden per Fax verfügbar, sondern können – bei initial vorhandener Internetverbindung – auf jedem Tablet ortsunabhängig gelesen werden.

Im Gegensatz zum Online-Client hält der Offline-Client sämtliche Gebäudedaten lokal auf dem Gerät vor und setzt entsprechend leistungsfähige Geräte voraus. Das Offline-Vorhalten der Daten erfolgt dabei vollständig verschlüsselt. Eine Sichtbarkeit der Daten für Nutzer wird erst durch einen einsatzbezogenen Freischaltcode der Leitstelle ermöglicht. Dieser wird per Datenverbindung automatisiert an die Endgeräte übertragen, beispielsweise per Mobilfunkdatenverbindung. Als

Rückfallebene bietet der Offline-Client darüber hinaus die Möglichkeit, den Freischaltcode per Hand in der Oberfläche des Offline-Clients einzugeben. Voraussetzung hierfür ist, dass dieser zuvor auf alternativen Übermittlungswegen (z.B. per Funk, Telefon) außerhalb des DSRS an die Einsatzkraft vor Ort übermittelt wurde.

3.6 Online-Client

Der Online-Client ist die Onlineversion der Einsatzanwendung und damit die Anwendung, die im Einsatzfall Daten zu einem Gebäude auf Tablets oder Laptops der Einsatzleitung anzeigt.

Der Online-Client ist mittels Internetzugang während eines Einsatzes mit dem DSRS verbunden und bietet den Zugriff auf den jeweils aktuellen Datenbestand. Eine Synchronisation ist nicht notwendig.

Der Online-Client stellt die folgenden Informationen zu Gebäuden zur Verfügung:

- Digitaler Alarmzettel
- Textgebundene Gebäudeinformationen
- Ansichten
- Lagepläne sowie Kartenmaterial von Google Maps
- Grundrisse

Im Gegensatz zum Offline-Client hält der Online-Client keine Daten lokal auf dem Gerät vor und setzt entsprechend weniger leistungsfähige Geräte voraus.

Der Zugriff auf die Daten erfolgt per Nutzerauthentifizierung (Benutzername, Passwort) und Freischaltung durch die Leitstelle.

3.7 Leitstellenanbindung

Um das DSRS möglichst effizient einsetzen zu können und die Gebäudedaten gegen unberechtigten Zugriff zu schützen, ist eine Anbindung an das Leitstellensystem der Feuerwehr empfehlenswert. Um auch ohne Leitstellenanbindung eine testweise Nutzung des DSRS zu ermöglichen, stellt der Auftragnehmer einen Leitstellensimulator zur Verfügung. Dieser ermöglicht per Weboberfläche die testweise Alarmierung von Einheiten zu fiktiven Einsätzen.

Wird eine Anbindung an die Leitstelle realisiert, wird im Einsatzfall seitens der Leitstelle ein Einsatz auf den Online- oder Offline-Clients der jeweils alarmierten Einheiten geöffnet und der Zugriff auf die entsprechenden relevanten Daten freigeschaltet. Bei der Anbindung an die Leitstelle werden Gebäudedaten auf dem Endgerät jeweils einzeln verschlüsselt. Im Falle eines Einsatzes wird von der Leistelle ein Freischaltcode über eine verschlüsselte Verbindung an die Anwendung gesendet, mit dem die einsatzrelevanten Daten für die Dauer eines Einsatzes bzw. eines definierten Zeitintervalls entschlüsselt werden. Alle Gebäudedaten, die nicht für einen Einsatz relevant sind, bleiben verschlüsselt. Eine Ausnahme hiervon stellen Zugriffe von Nutzern mit sogenanntem Disponentenrecht dar. Diese können auch ohne laufenden Einsatz Gebäudedaten aufrufen. Die Zuweisung der richtigen Rechte liegt in der Verantwortung des Auftraggebers.

Die Leitstellenanbindung ist integraler Bestandteil des Datensicherheits- und Datenschutzkonzeptes, welches die rechtskonforme Nutzungsmöglichkeit der Software absichert. Gleichzeitig verkürzt die Leistellenanbindung den Zeitraum zum Zugriff auf die Daten, indem Einsätze auf den Geräten bereits von der Leitstelle geöffnet werden können.

Ebenso ermöglicht erst die Anbindung an die Leitstelle das Bereitstellen des Digitalen Alarmzettels. Dieser beinhaltet u.a. das Alarmstichwort, die Einsatzadresse in Google Maps sowie die gleichzeitig alarmierten Einheiten.

Das DSRS ist bei der Leitstellenanbindung jedoch darauf angewiesen, dass die Leitstelle technische Schnittstellen zur Anbindung von externen Systemen zur Verfügung stellt. Hierzu zählen insbesondere die Möglichkeit zur Übertragung von Einsatzort (Adresse und Geokoordinate) sowie die Möglichkeit zur Übertragung der alarmierten Einheiten.

3.8 Einsatzübersicht / Zentralarbeitsplatzansicht

Um eine Nutzung der DSRS-Daten nicht nur für den abwehrenden Brandschutz an der Einsatzstelle zu ermöglichen, sondern auch für den Leitstellendisponenten selber, wird eine Web-Oberfläche mit Adress-Suchfunktion zur Verfügung gestellt, über die eine über entsprechende Berechtigung verfügende Person innerhalb der Leitstelle unter Dokumentation der Einsatznummer auf jeden Datensatz des der Feuerwehr zugewiesenen PLZ Bereichs zugreifen kann. So wird sichergestellt, dass die Leitstelle sich Daten für jeden Einsatz anzeigen lassen kann, selbst wenn die an der Einsatzstelle eingesetzten Kräfte keine Nutzer des Smart Rescue Systems sind (beispielsweise ein Rettungsdiensteinsatz) oder eine Einsatzstelle eine Recherche an anderer Stelle in der Stadt nach sich zieht (beispielsweise Turnhalle als Notfallquartier in Stadtteil X aufgrund von Bombenfund in Stadtteil Y).

3.9 Kartenansichten

An verschiedenen Stellen bietet das DSRS den Zugriff auf Kartenmaterial von Google Maps. Der Zugang zu diesem Service sowie auf dieses Kartenmaterial im Rahmen von DSRS ist Teil des Lieferumfangs.

Für die inhaltliche Korrektheit und Aktualität dieses Kartenmaterials kann seitens des Auftragnehmers keine Gewähr übernommen werden. Kartenmaterial wird im DSRS so genutzt, wie es vom Kartenanbieter übermittelt (as-is) wird. Es gelten dabei die vom Kartenbieter vorgegebenen Bedingungen, die eine Nutzung im Rahmen des DSRS jedoch nicht einschränken.

Eine offlinefähige Kartenfunktion ist nicht Gegenstand des Vertrags.

3.10 Fortlaufender Betrieb des Dräger Smart Rescue System

Der fortlaufende Betrieb beinhaltet folgende Elemente:

Technischer Betrieb

Der Auftragnehmer übernimmt den technischen Betrieb der Anwendung DSRS und stellt diese Anwendung dem Auftraggeber zur Nutzung zur Verfügung.

Der technische Betrieb umfasst den Betrieb der Anwendung und seiner Serviceinfrastruktur in Rechenzentren in der Europäischen Union. Diese Serviceinfrastruktur umfasst alle Komponenten zum Betrieb der Onlineversion der Anwendung, Anbindung der Offline-Client, Datenverwaltungsbackend, Mandantenverwaltung, DSRS-seitige Schnittstellen zum Zugriff auf Leitstellenschnittstellen sowie Schnittstellen zum Kartenanbieter Google Maps.

Der technische Betrieb deckt alle Komponenten ab, die zum Betrieb der Anwendung notwendig sind, also Server, Datenspeichersysteme, Netzwerkanbindungen, Backup und Sicherheitsinfrastruktur wie etwa Verschlüsselungstechnologien.

Der Auftraggeber muss hierzu keine Komponenten selbst betreiben außer den Einsatzgeräten (Tablet, Laptop), auf denen die Anwendung genutzt werden soll, sowie die zum Zugriff notwendigen Netzwerke wie z.B. mobiles Internet. Eine passende Dimensionierung dieser Geräte obliegt dem Auftraggeber.

Support
Im Rahmen der kostenlosen Erprobung hat der Aufttraggeber jederzeit die Möglichkeit, über die Webseite www.smart-rescue.info und die dort befindliche Kontaktmöglichkeit eine Supportanfrage an den Dräger Helpdesk zu stellen.

Der Helpdesk bildet den sogenannten First-Level-Support ab. Darüber hinaus betreibt der Auftragnehmer einen Second-Level- (Expertenebene) und Third-Level-Support (Entwicklungsebene). Second- und Third-Level werden durch den First-Level-Support eingebunden, wenn Anfragen nicht direkt durch den First-Level-Support gelöst werden können.

Der Leistungsumfang des First-Level-Supports beinhaltet die folgenden Punkte:

- Unterstützung von Anwendern bei Problemen während der Nutzung und Bedienung der Anwendungen
- Annahme, Klassifizierung und Weiterleitung von Störungsmeldungen an den Second-Level-Support

4 Systemvoraussetzungen

Das DSRS ist ein Cloud basiertes System und besteht aus mehreren Komponenten, die sowohl online über das Internet, als auch lokal auf einem Endgerät zum Einsatz kommen. Die Online-Komponenten werden in der Microsoft Azure Cloud in Europa betrieben.

Zur Nutzung aller Online-Anwendungsteile, also beispielsweise der Feuerwehr Online-Client oder die Datenverwaltung, sind ein Internetzugang und ein gängiger Webbrowser in einer aktuellen Version notwendig. Gängige Webbrowser sind Microsoft Edge, Mozilla Firefox oder Google Chrome.

Die Nutzung mit älteren Versionen dieser Browser ist technisch mit gegebenenfalls entstehenden Einschränkungen und Leistungsverlusten möglich. Eine Nutzung mit älteren Browsern wird von Dräger nicht empfohlen.

Bei dem Offline-Client handelt es sich im um eine Anwendung, die lokal auf einem Endgerät installiert wird und als Einsatzanwendung für Rettungskräfte konzipiert ist.

Bei dem mit DSRS verwendeten Endgerät sollte es sich um ein touchfähiges Gerät, also einen Tablet-Computer, handeln. Eine Bedienung ohne Touchscreen wird nicht empfohlen.

Als Betriebssystem wird Windows 10 (64 Bit) vorausgesetzt. Eine Nutzung auf älteren Windows 8 Geräten muss im Einzelfall geprüft werden. Gegebenenfalls kann es zu Einschränkungen und Leistungsverlusten kommen. Die Geräte sollten mindestens über 4 GB RAM und 64 GB verfügbaren Festplattenspeicherplatz sowie einer Displayauflösung von 1024 x 768 verfügen. Bei geringeren Werten ist mit Einschränkungen des lokal verfügbaren Datenbestandes zu rechnen.

Weiterhin kann der Offline Client auf den meisten marktüblichen iOS und Android Tablets genutzt werden.

Auch der sogenannte Offline-Client benötigt einen Internetzugang zur Synchronisierung von Daten, sowie zur Aktivierung von Einsätzen. Nach erfolgreicher Synchronisierung und Aktivierung kann das Gerät für die Dauer eines Einsatzes offline verwendet werden. Im Notfall kann die Einsatzaktivierung auch im Offlinemodus durchgeführt werden, dies ist jedoch mit Usability-Einschränkungen verbunden.

Daher wird empfohlen, die Endgeräte für den Einsatz durch Rettungskräfte mit einer Mobilfunkverbindung über eine integrierte SIM-Karte auszustatten.

5 Datenschutz und Datensicherheit

Das DSRS ist dazu geeignet, datenschutzkonform genutzt zu werden. Ob die Verarbeitung der Daten für die Ausübung der hoheitlichen Maßnahmen im Einzelfall rechtmäßig ist, ist eine Bewertung, für die Dräger nicht verantwortlich ist und der jeweiligen Einsatzfunktion bzw. der Feuerwehr obliegt. Insoweit gilt für die Nutzung des DSRS das gleiche wie für andere in Einsatzfällen herangezogene Informationsquellen, die einen gewissen Personenbezug aufweisen. Das DSRS ist aber insbesondere durch seine Verschlüsslungstechnologien und die Vorgaben des einsatzbezogenen Einzelfallabrufs auf eine möglichst geringe Eingriffsintensität ausgelegt, um die Rechtfertigung nach den einschlägigen Verfahrensvorschriften der Einsatzkräfte zu unterstützen.

Dem Auftraggeber obliegt die Sicherstellung von organisatorischen Maßnahmen zur datenschutzkonformen Verwendung der Anwendung und Daten durch Behörden und Organisationen mit Sicherheitsaufgaben.

Alle Gebäudeinformationen im DSRS werden nach dem Stand der Technik vor unberechtigten Zugriffen durch die folgenden technisch-organisatorischen Maßnahmen geschützt:

- **Auf dem Server:**
  Die Gebäudedaten werden über einen gesicherten Server in mehreren Rechenzentren in Europa nach europäischem Datenschutzrecht gespeichert. Die zentrale Server-Infrastruktur, wie Speicherplatz und Rechnerleistung, verantwortet ein renommierter Cloud Provider (ein Anbieter für Dienstleistung über das Internet). Dieser Cloud Provider arbeitet nach höchsten Sicherheitsstandards. Er ist damit in der Branche führend. Seine Rechenzentren sind nach den gängigen internationalen (z. B. ISO27001, ISO27018, CSA STAR) wie nationalen Standards (z. B. BSI IT Grundschutz oder UK Cyber Essentials Plus) zertifiziert.
- **Zwischen Server und Endgeräten:**
  Sobald Informationen vom gesicherten Server auf die Tablets (oder andere Endgeräte) der Einsatzkräfte fließen, werden sie verschlüsselt – ganz gleich, ob die Daten aktiv abgerufen oder die Systeme im Hintergrund synchronisiert werden.
- **Auf den Endgeräten:**
  Auf den Endgeräten wie beispielsweise den Tablets werden die Gebäudeinformationen von dem Offline-Client gespeichert. Dabei handelt es sich um ein Computerprogramm, das mit dem gesicherten Server kommuniziert. Dieses Programm stellt sicher, dass Einsatzkräfte auch ohne Verbindung zum Internet auf die Daten zugreifen können. Gleichzeitig sind die Daten durch das Programm vor unberechtigten Zugriffen geschützt. Bei einem Einsatz sendet die Leitstelle über eine verschlüsselte Verbindung einen Freischalt-Code an die DSRS-App auf die Endgeräte der Rettungskräfte. Damit werden nur die Daten entschlüsselt, die für den Einsatz relevant sind. Alle anderen Gebäudedaten bleiben verschlüsselt.

6 Daten des Auftraggebers, Nutzung und Verantwortlichkeit

Der Auftraggeber erhält Zugang zum Bereitstellen und Hochladen von Informationen, beispielsweise von textgebundenen Gebäudeinformationen oder bildgebundenen Plänen und Gebäudeansichten.

Der Auftraggeber strebt dabei an, dass alle Informationen richtig und aktuell sind, übernimmt aber gegenüber dem Auftragnehmer keine Gewähr für Richtigkeit oder Aktualität der weitergegebenen Informationen.

Der Auftraggeber gewährleistet jedoch, dass er zur Weitergabe und Nutzung der übergebenen Informationen berechtigt ist und über diese in dem für die Durchführung dieses Vertrags nötigen Umfang verfügen kann. Der Auftragnehmer ist nicht dazu verpflichtet, dass vorstehende zu prüfen und ist für die vorstehenden Bedingungen nicht verantwortlich.

Der Auftragnehmer wird durch den Auftraggeber berechtigt, während der Laufzeit die Informationen in jeder Weise zu verwenden, die für die Erreichung des Vertragszwecks dienlich sind. Hiervon umfasst ist insbesondere das Recht:

- die Informationen mit anderen Elementen, oder weiteren Informationen, die nicht Gegenstand der vertraglichen Vereinbarung zwischen Auftraggeber und Auftragnehmer sind, zu verknüpfen, zu poolen, zu verbinden, zu vermischen oder gemeinsam zu verwenden.
- von den Informationen weitere Erkenntnisse abzuleiten und die Informationen auszuwerten.
- die Informationen an Dritte zur Förderung des Vertragszwecks oder Weiterentwicklung zu diesem Zweck weiterzugeben, was insbesondere für an der Weiterentwicklung beteiligten Feuerwehren und Bildungs- und Forschungseinrichtungen gilt, die die Nutzbarkeit der Informationen für sicherheitstechnische Zwecke zusammen mit Dräger evaluieren.
- die Informationen nach Ermessen von Dräger zu bearbeiten, zu verändern, zu veredeln oder neu zu strukturieren.
- die Informationen in Software oder andere digitale Verarbeitungssysteme einzufügen und zusammen hiermit zu nutzen oder zur Nutzung im Rahmen der Produktnutzung anzubieten.

Sofern die Informationen urheberrechtlich geschützt sind, räumt der Auftraggeber dem Auftragnehmer ein nicht-exklusives, zeitlich auf die Dauer des Vertrags beschränktes, räumlich jedoch unbeschränktes Nutzungsrecht für alle die Nutzungen ein, die typischerweise mit einer Nutzung zu den oben in dieser Ziffer genannten Zwecken und zur Umsetzung dieses Vertrags einhergehen.

Der Auftragnehmer übernimmt keine Gewähr für die technische Integrität der Daten oder für deren Verlust bzw. deren Verfügbarkeit, soweit letzteres nicht ausdrücklich vereinbart ist. Die Datensicherung obliegt dem Auftraggeber. Im Zusammenhang mit der zugrunde liegenden IT-Infrastruktur ergibt sich der Leistungsumfang aus den Bedingungen des IT-Infrastrukturanbieters (Cloud-Provider).
Die entsprechenden Bedingungen sind verfügbar unter (bitte wählen Sie Ihre Sprache und die für EU-Kunden relevanten Bedingungen, denn so kaufen wir die Azure Cloud Infrastructure).

für SLA
https://www.microsoft.com/en-us/licensing/product-licensing/products

für die Bedingungen des Online-Service
https://www.microsoft.com/en-us/licensing/product-licensing/products

7 Sonstige Leistungsparameter und Rechtliche Rahmenbedingungen

Die angeboten und in der Cloud gehosteten Leistungen sowie die sonstigen Eigenschaften des DSRS bedingen eine Einbettung in eine bestehende IT-Landschaft. Naturgemäß sind die konkreten Bedingungen einer bestimmten IT-Landschaft nicht allgemein vorhersehbar. Etwaige Anpassungen und konkrete Implementierungsmaßnahmen sind daher nicht Bestandteil des Leistungsumfangs der des DSRS. Die weitere bzw. integrierte Nutzung auf kostenpflichtiger Basis kann daher die Begleitung durch ein Implementationsprojekt voraussetzen. Gleichfalls können die vertraglichen Parameter einer längerfristigen Beschaffung von der Beschaffungsmethode abhängig sein. Der Auftragnehmer behält sich auch vor diesem Hintergrund vor, Abweichungen von den angebotenen Bedingungen vorzusehen,

sofern individuelle Implementierungen nötig sind oder die Beschaffung in einer anderen Weise geschieht, als durch einen Vertragsschluss mittels Bestellformular oder Angebot von uns an Sie.

Als Cloud-basierte IT-Plattformanwendung werden dabei die hinsichtlich der Cloud-Infrastruktur marktüblichen Bedingungen inkludiert, die weitestgehend vom Cloud Provider vorgegeben werden. Dies betrifft insbesondere die Parameter Service-Level in Bezug auf die Cloud-Infrastruktur, die Verantwortlichkeit für Nutzungshandlungen, zugesicherte Eigenschaften der Infrastruktur und Leistungsstörungsfolgen.

Wie bei Dritt-Daten-basierten Plattformanwendungen üblich, kann für diese Daten hinsichtlich ihrer Konsistenz und Qualität keine Verantwortung übernommen werden, was insbesondere auch in der Testphase gilt. Eine Prüfung der bereitgestellten Daten gehört nicht zum Leistungsumfang und ist faktisch weder sinnvoll möglich noch wirtschaftlich abbildbar. Als zusätzliche Informationsquelle im Einsatzfall dienen die bereitgestellten Daten als Einsatzunterstützung, ersetzen aber nicht das Vorgehen entsprechend der Einsatzregeln. Über die Plattform können die Daten in der Qualität abgerufen werden, wie sie von den beteiligten Dritten oder dem Auftraggeber zur Verfügung gestellt werden. Den Beteiligten ist dabei bewusst, dass eine Haftung für die Datenqualität von Dräger Seite nicht übernommen werden kann. Gleichfalls kann eine Verantwortung für die Integrität und die Verfügbarkeit der Daten nur insoweit übernommen werden, wie dies im Verhältnis zum Infrastruktur-Anbieter vereinbart ist. Dräger kann insoweit nicht gewährleisten, dass etwaige in der Cloud Plattform abgelegten Daten dort unbeschädigt bleiben, nicht verloren gehen oder wiederherstellbar sind. Dräger wird die mit dem Infrastrukturanbieter vertraglich vereinbarten Wiederherstellungsversuche durchführen, wenngleich eine erfolgreiche Widerherstellung durch Dräger nicht geschuldet ist.

In Ergänzung zum Vorstehenden gelten die nachfolgenden Bedingungen:

Rechteeinräumungen
Der Auftraggeber räumt Dräger hiermit für die Dauer der Nutzung des DSRS ein einfaches, nicht übertragbares, lediglich an verbundene Unternehmen des Auftragnehmers oder im seinem Interessenbereich tätige Dritte unterlizensierbares Recht ein, die Daten und das geistige Eigentum des Auftraggebers zu nutzen, soweit dies zur Erbringung der Leistungen gegenüber dem Auftraggeber erforderlich oder in dieser Vereinbarung vorgesehen ist. Dies beinhaltet insbesondere auch die Weitergabe der Daten an andere Behörden mit öffentlichen Sicherheitsaufgaben, welche im Rahmen der berechtigten Erfüllung hoheitlicher Aufgaben im Einsatzfall auf die Datenbestände zugreifen, beispielsweise weil der Einsatz im geografischen Bereich des Auftraggebers stattfindet. Soweit der Auftraggeber gemäß den Regelungen dieser Vereinbarung selbst dafür verantwortlich ist, Hardware, Software oder sonstige Materialien Dritter inklusive Daten beizustellen („Beigestelltes Dritt-IP“), räumt der Auftraggeber Dräger hiermit für die Dauer der Nutzung des DSRS ein einfaches, nicht übertragbares, lediglich an verbundene Unternehmen des Auftragnehmers oder im seinem Interessenbereich tätige Dritte unterlizensierbares Recht ein, das Beigestellte Dritt-IP zu nutzen, soweit dies zur Erbringung der Leistungen gegenüber dem Auftraggeber erforderlich oder in dieser Vereinbarung vorgesehen ist.

Dabei stellt der Auftraggeber sicher, dass der Kunde im Verhältnis zum jeweiligen Rechteinhaber berechtigt und in der Lage ist, Dräger alle zur Erbringung der Leistungen oder in dieser Vereinbarung vorgesehen erforderlichen Nutzungsrechte an dem Beigestellten Dritt-IP einzuräumen.

Dräger räumt dem Kunden für die Dauer der Laufzeit dieser Vereinbarung das einfache, nicht unterlizensierbare Recht ein, das von Dräger bereitgestellte geistige Eigentum in dem Umfang zu nutzen, wie es für die Realisierung der hier getroffenen Vereinbarung nötig ist. Dazu stellen die Parteien klar, dass unter diesem Vertrag, insbesondere im Bereich der SaaS-Services grundsätzlich keine Überlassung von Kopien der bei dem IT-Infrastruktur-Betreiber betriebenen und im Rahmen

dieses Vertrags genutzten Software an den Auftraggeber geschuldet ist, soweit nicht im Rahmen dieser Vereinbarung ausdrücklich etwas anders vereinbart ist.

Open Source Software
Das DSRS enthält bestimmte Open Source Software. Open Source Software unterliegt regelmäßig besonderen Lizenzbedingungen, die in ihrem Umfang vorrangig gelten. Die betreffenden Lizenzen beziehen sich auf die jeweils zugehörigen Open Source Software Elemente. Diese Lizenzen beinhalten unter anderem Haftungsbeschränkungen zu Gunsten der Software-Urheber und Aussagen darüber, wie mit den betreffenden Open Source Software Elementen verfahren werden darf. Häufig wird das Recht zur Nutzung dieser Elemente von den Software-Urhebern direkt dem Endkunden eingeräumt. Aus den Open Source Lizenzbestimmungen ergeben sich keine aktiv vorzunehmenden Handlungen des Endkunden. Weitere Informationen, wie z.B. die Lizenzbestimmungen, zu der in diesem Produkt eingesetzten Open Source Software stehen unter folgender Internetseite: https://www.smart-rescue.info/downloads-1.

Gewährleistungen
Falls Sie das DSRS kostenlos nutzen, übernimmt der Auftragnehmer keine Gewährleistung für eine bestimmte Funktionalität, Marktfähigkeit, Eignung für einen bestimmten Zweck, Nichtverletzung von Drittrechten, Verfügbarkeit oder Service Level, außer, dass die Bereitstellung der Leistungen den geltenden Gesetzen entspricht, soweit die Überwachung der Vereinbarkeit mit diesen dem Pflichtenkreis des Auftragnehmers zugeordnet ist.

Sofern Sie das DSRS gegen Entgelt verwenden gelten die allgemeinen gesetzlichen Gewährleistungsvorschriften.

Haftungsbeschränkung
Sollte der Auftragnehmer das DSRS kostenlos erhalten (z.B. im Rahmen einer Testversion), haftet der Auftragnehmer nur für vorsätzliches Fehlverhalten und direkte Schäden bis zu einem Höchstbetrag von 1.000,00 EUR.

Sofern für die Nutzung des DSRS ein Entgelt vereinbart ist, gilt das Nachfolgende: Die Parteien haften einander nach den allgemeinen gesetzlichen Vorschriften, soweit sich aus den nachfolgenden Regelungen nicht etwas anderes ergibt.

Die Bestimmungen gelten für alle Schadensersatz- und Aufwendungsersatzansprüche, gleich aus welchem Rechtsgrund.

Inhalt der Haftungsbeschränkung:

a) Für Personenschäden (Verletzung von Leben, Körper und Gesundheit), im Fall von Vorsatz sowie im Falle einer Haftung nach dem Produkthaftungsgesetz haftet Dräger unbeschränkt nach den gesetzlichen Bestimmungen.
b) Für grob fahrlässig verursachte Schäden innerhalb eines Zwölfmonatszeitraums ist die Haftung von Dräger der Höhe nach insgesamt auf einen Betrag von 50.000 EUR beschränkt.
c) Für sonst fahrlässig verursachte Schäden ist die Haftung der Höhe nach insgesamt auf einen Betrag von 10.000 EUR beschränkt. Darüber hinaus ist im Fall der sonstigen Fahrlässigkeit die Haftung für Folgeschäden ausgeschlossen.
d) Soweit die Haftung von Dräger gegenüber dem Auftraggeber auf einer Verletzung von Vertragspflichten in Bezug auf die IT-Infrastruktur Services beruht, ist die Haftung von Dräger – unbeschadet der weitergehenden Haftungsbeschränkungen dieser Regelungen auf die Ansprüche beschränkt, die Dräger gegenüber dem IT-Infrastruktur Betreiber durchsetzen kann. Die betreffenden Bedingungen sind abrufbar unter:

- für SLA: http://www.microsoftvolumelicensing.com/SLA
- für OST: http://go.microsoft.com/?linkid=9840733

e) Dräger haftet für den Verlust von Daten nur insoweit, als der Kunde durch übliche Sicherungsverfahren sichergestellt hat, dass die Daten aus Datenmaterial, das in maschinenlesbarer Form bereitgehalten wird, mit vertretbarem Aufwand rekonstruiert werden können. Im Übrigen gelten auch beim Verlust von Daten die vorstehenden Haftungsbeschränkungen.
f) Im Übrigen haften die Parteien einander nach den allgemeinen gesetzlichen Vorschriften.

Datenschutz
Der Auftragnehmer wird personenbezogene Daten im Sinne der Datenschutzgrundverordnung (DSGVO) und anderer einschlägiger Datenschutzbestimmungen (zusammen ab hier „Daten“) nur nach Maßgabe der jeweils einschlägigen gesetzlichen Bestimmungen erheben, verarbeiten und nutzen.

Der Auftragnehmer ist Verantwortlicher gem. Art. 24 der Datenschutzgrundverordnung (DSGVO). Der Auftraggeber und Auftragnehmer sind keine gemeinsamen Verantwortlichen im Sinne des Art. 26 DSGVO.

Sie bestimmen jeder für sich und unabhängig voneinander über die Mittel und Zwecke der Verarbeitung in ihrem Verantwortungsbereich.

Der Auftragnehmer ist in seinem Verantwortungsbereich verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen dieser Vereinbarung durchgeführten Verarbeitung und Nutzung der Daten, die ihm zur Vertragserfüllung durch den Herausgeber zur Verfügung gestellt werden, so im Hinblick auf die Regelungen der Datenschutzgrundverordnung und anderer Vorschriften über den Datenschutz.

Er hat in eigener Verantwortung die formalen Datenschutzvorschriften (z.B. Bestellung eines betrieblichen Datenschutzbeauftragten, Führung von Dokumentationen) und die Rechte der Betroffenen (z.B. Benachrichtigung über die Speicherung, Auskunftserteilung) wahrzunehmen.

Der Auftragnehmer ist verpflichtet, die Daten ausschließlich bestimmungsgemäß, d.h. soweit dies zur ordnungsgemäßen Erfüllung des Vertrages erforderlich ist und nur für die Zwecke zu verwenden, die nach diesem Vertrag gestattet sind. Die übermittelten Daten werden nicht für eigene oder andere Zwecke benutzt und nicht an Dritte weitergegeben, sofern die Weitergabe nicht im Rahmen des Vertragsverhältnisses vorgesehen ist. Eine Zweckänderung für Zwecke, die außerhalb dieser Vereinbarung liegen, ist ausgeschlossen.

Der Auftragnehmer verpflichtet sich, zur Erbringung der vertragsgegenständlichen Leistungen nur Mitarbeiter einzusetzen, die durch geeignete Maßnahmen mit den gesetzlichen Vorschriften über den Datenschutz und den speziellen datenschutzrechtlichen Anforderungen dieses Vertrags vertraut gemacht sowie zur Vertraulichkeit und der Wahrung von Geschäfts- und Betriebsgeheimnissen der beteiligten Parteien, verpflichtet wurden.

Der Auftragnehmer hat - soweit gesetzlich vorgeschrieben - einen Datenschutzbeauftragten zu bestellen. Dessen Kontaktdaten werden dem Herausgeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

Der Auftragnehmer sichert zu, Maßnahmen zum Schutz der Daten, die im Rahmen der vertragsgegenständlichen Leistungen erhoben, verarbeitet oder genutzt werden, entsprechend Art. 64 DSGVO zu treffen und diese auf Anfrage unentgeltlich nachzuweisen, sowie spezifische Maßnahmen insbesondere im Hinblick auf die Art des Datenaustauschs/Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand zu treffen.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen des Vereinbarung im Verantwortungsbereich des Auftragnehmers erleidet, ist dieser gegenüber dem Betroffenen verantwortlich.

Diese Bestimmungen gelten entsprechend für Daten, die der Auftragnehmer für den Auftraggeber bei der Erbringung der vertragsgegenständlichen Leistungen erhebt, sowie für Verarbeitungs- und Nutzungsergebnisse in Bezug auf personenbezogene Daten, die der Auftragnehmer für den Auftraggeber bei der Erbringung der vertragsgegenständlichen Leistungen erzielt.

Im Übrigen ist der Auftraggeber für die Nutzung etwaiger Daten im Zusammenhang mit der vertragsgegenständlichen Plattformlösung und die daraus hervorgehenden Verarbeitungsvorgänge verantwortlich.

Leistungsort
Leistungsort für die von Dräger zu erbringenden SaaS-Services ist der Standort des Internet-Servers des IT-Infrastruktur Betreibers soweit nicht etwas anderes vereinbart ist. Übergabepunkt für die Leistungen von Dräger an den Auftraggeber im Rahmen der Erbringung der SaaS-Services ist der Routerausgang des Servers des IT-Infrastruktur Betreibers. Dräger ist für das vertragsgemäße Funktionieren der von Dräger selbst oder ihren Erfüllungsgehilfen betriebenen Systeme, Rechner und Leitungen verantwortlich.

Der Auftraggeber ist für die Schaffung der erforderlichen kundenseitigen Nutzungsvoraussetzungen, insbesondere die Systemvoraussetzungen, Infrastruktur sowie für die Telekommunikationsverbindung zwischen dem Auftraggeber und Dräger bis zum Übergabepunkt verantwortlich. Er wird dem Stand der Technik entsprechende technische und organisatorische Sicherheitsstandards einhalten und dafür sorgen, dass von seinen Systemen keine Viren in die Systeme von Dräger gelangen.

Sonstiges
Die Vertragspartner verpflichten sich, sämtliche Daten und Informationen, die sie von dem jeweils anderen Vertragspartner erhalten, streng vertraulich zu behandeln und ohne vorherige schriftliche Zustimmung des jeweils anderen Vertragspartners nicht an Dritte weiterzugeben, sofern die Weitergabe nicht im Rahmen des Vertragsverhältnisses vorgesehen ist.

Dräger schuldet grundsätzlich nur die in diesem Angebot konkret spezifizierten Leistungen. Eine weitergehende Pflicht etwa zur Erbringung allgemeiner Aufklärungs- oder Beratungsleistungen besteht nicht, soweit diese nicht ausdrücklich vereinbart worden ist.

Unbeschadet etwaiger Kündigungsrechte ist Dräger auch dann zur außerordentlichen Kündigung der betreffenden Leistung berechtigt, wenn der IT-Infrastruktur Betreiber, von dem Dräger IT-Infrastruktur Services bezieht, den zugrundeliegenden Vertrag kündigt oder seine Leistungen gegenüber Dräger einstellt.

Dräger wird die Software-Spezifikationen nach eigenem Ermessen aktualisieren und an gesetzlich zwingende Änderungen anpassen. Sofern und soweit mit der Bereitstellung einer neuen Version der Software oder einer sonstigen Änderung der Software-Spezifikationen, einer Änderung von Funktionalitäten der Software einhergeht, wird Dräger dies dem Auftraggeber spätestens vier (4) Wochen vor dem Wirksamwerden einer solchen Änderung per E-Mail oder in sonst geeigneter Weise ankündigen. Widerspricht der Kunde der Änderung nicht schriftlich innerhalb einer Frist von zwei (2) Wochen ab Zugang der Änderungsmitteilung, wird die Änderung Vertragsbestandteil. Widerspricht der Kunde, kann Dräger die betreffende Leistung mit einer Frist von drei (3) Monaten kündigen, wobei Dräger bis zum Ablauf der Kündigungsfrist die alte Version der Software mit den bisherigen Software-

Spezifikationen zur Verfügung stellen wird. Im Falle einer kostenlosen Nutzung des DSRS durch den Auftraggeber beträgt diese Kündigungsfrist zwei Wochen.

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein, so wird die Gültigkeit der übrigen Bestimmungen dadurch nicht berührt. Anstelle der unwirksamen Bestimmung soll eine Regelung gelten, die dem am nächsten kommt, was die Vertragspartner gewollt haben oder gewollt hätten, wenn ihnen die Unwirksamkeit der Bestimmung bekannt gewesen wäre. Dasselbe gilt für etwaige Vertragslücken.

Mündliche Nebenabreden zu diesem Vertrag bestehen nicht. Änderungen und/oder Ergänzung dieses Vertrages bedürfen der Schriftform. Dies gilt auch für das vorstehende Schriftformerfordernis. Gerichtsstand ist Lübeck. Dräger ist nach eigenem Ermessen berechtigt, auch das für den Sitz des Vertragspartners zuständige Gericht in Anspruch zu nehmen.

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

Der Gegenstand dieses Vertrages ist die datenschutzgerechte Erledigung aller für den Auftraggeber der im Vertrag über die Nutzung des Dräger Smart Rescue System („Hauptvertrag“) vereinbarten Leistungen. Hierzu werden nachfolgende Vereinbarungen getroffen:

1. Anwendungsbereich

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

- Einsatzbezogene Bereitstellung eines Digitalen Alarmzettels
- Einsatzbezogene Bereitstellung von Gebäudedaten und -plänen
- Einsatzbezogene Bereitstellung von Plänen zu örtlicher Infrastruktur

beauftragt. Dabei ist nicht auszuschließen, dass der Auftragnehmer im Zuge der vertragsgemäßen Durchführung der Leistungen die Möglichkeit des Zugriffs auf personenbezogene Daten, die vom Auftraggeber als Verantwortlichem dieser Daten oder aus der Sphäre des Auftraggebers stammen (nachfolgend: „Auftraggeberdaten“), hat und diese verarbeiten wird.

1.2. Dieser Vertrag über die Auftragsverarbeitung enthält die dabei zu beachtenden allgemeinen Anforderungen und gilt für alle Datenverarbeitungsaufträge des Auftraggebers an den Auftragnehmer. 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:

- Beschäftigtendaten
- Einsatzbezogene Daten

Von der Verarbeitung betroffen sind folgende Personengruppen

- Beschäftigte
- An Einsätzen beteiligte Dritte (z.B. Zeugen, Geschädigte)

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer beachtet bei der Verarbeitung von Auftraggeberdaten die am Sitz des Auftraggebers geltenden Datenschutzgesetze und in jedem Fall mindestens die Anforderungen der Datenschutzgrundverordnung (DS-GVO), soweit diese für Leistungen des Auftragnehmers gilt, insbesondere Art. 28 DS-GVO. 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 gesetzlichen Anforderungen des Datenschutzes gerecht wird.

3.2. Der Auftragnehmer verarbeitet Auftraggeberdaten nur im Rahmen des Auftrags und entsprechend den schriftlichen Weisungen des Auftraggebers. Der Auftraggeber ist und bleibt als speichernde und verantwortliche Stelle der „Herr der Daten“.

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

3.4. Der Auftragnehmer 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 an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.5. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Vorschriften über den Datenschutz verstößt, weist der Auftragnehmer den Auftraggeber in Textform 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. Der Auftragnehmer unterrichtet den Auftraggeber außerdem unverzüglich, wenn eine Aufsichtsbehörde ihm gegenüber tätig wird und das Vorgehen die Auftragsverarbeitung aus dieser Vereinbarung betrifft.

3.6. Der Auftragnehmer ist verpflichtet, bei der Verarbeitung von Auftraggeberdaten ausschließlich Personal einzusetzen, das zur Vertraulichkeit verpflichtet wurde und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurde. Der Auftragnehmer und jede dem Auftragnehmer 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 Auftragnehmer 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 Auftragnehmer wird nach Abschluss der Vertragsbeziehung alle personenbezogenen Daten zurückgeben oder, nach Absprache mit dem Auftraggeber, löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.9. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben. Der Auftragnehmer 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 Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten,

Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören

- die 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 und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

3.11. Der Auftragnehmer 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 Auftragnehmer ermittelt.

3.12. 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

3.13. Der Auftragnehmer 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.

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 Auftragnehmer 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 Auftragnehmer 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 stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.

4.3. Werden Subunternehmer bzw. Unterauftragsdatenverarbeiter eingesetzt, gewährleistet der Auftragnehmer 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 Unterauftragnehmer.

4.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer 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

5.1. Der Auftraggeber beurteilt die Zulässigkeit der Verwendung von Auftraggeberdaten durch den Auftragnehmer im Rahmen des Auftrags gemäß den Regelungen der DS-GVO und anderer anzuwendender Vorschriften über den Datenschutz. Der Auftraggeber stellt sicher, dass die Auftraggeberdaten zweifelsfrei aus dem Herrschaftsbereich des Auftraggebers stammen und ordnungsgemäß erhoben wurden bzw. werden.

5.2. Der Auftraggeber wird den Auftragnehmer unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten unterrichten, insbesondere bei der Prüfung der Ergebnisse der Auftragsdatenverarbeitung.

5.3. Der Auftraggeber wahrt die Rechte der Betroffenen. Der Auftraggeber ist für die Informationspflichten gegenüber Dritten verantwortlich, insbesondere nach Art. 33, 34 DS-GVO. Der Auftragnehmer unterstützt den Auftraggeber bei dieser Pflicht durch zur Verfügungstellung der erforderlichen Informationen.

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

5.5. Soweit der Auftraggeber die Auftraggeberdaten selbst als Auftragsverarbeiter für einen Dritten verarbeitet und die Tätigkeit des Auftragnehmers daher eine Unterauftragsdatenverarbeitung darstellt, stellt der Auftraggeber 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 Auftraggeber beauftragt den Auftragnehmer in diesen Fällen nur, wenn er zuvor die Genehmigung des Dritten eingeholt hat. Er stellt außerdem sicher, dass dem Auftragnehmer die gleichen Datenschutzpflichten auferlegt werden, wie dem Auftraggeber selbst aus dem Auftragsverarbeitungsvertrag mit dem Dritten auferlegt sind. 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.

5.6. 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 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 oder der Auftragnehmer eine ihn aus Art. 82 Abs. 2 Satz 2 DS-GVO treffende Pflicht schuldhaft verletzt.

5.7. 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.

6. Besonders geschützte Daten, Patientendaten, Arzt-/Patientengeheimnis

6.1. Die Regelungen dieser Ziff. 6 gelten vorrangig für den Umgang mit besonders geschützten Daten i.S.d. Art. 9 DS-GVO, insbesondere für Gesundheitsdaten, für Patientendaten i.S.d. jeweils einschlägigen Krankenhausgesetzes sowie für Daten, die unter das Arzt-/Patientengeheimnis i.S.d. § 203 StGB fallen können („Besondere Auftraggeberdaten“).

6.2. Der Auftraggeber wird dafür Sorge tragen, dass der Auftragnehmer bei der Durchführung der vertraglichen Leistungen keinen Zugriff auf besondere Auftraggeberdaten hat. Dazu zählen z.B. Untersuchungsbefunde oder Daten, die diesen Befunden zugrunde liegen. Insoweit eine Zugriffsmöglichkeit auf solche besonderen Auftraggeberdaten nicht verhindert werden kann, stellt der Auftraggeber durch geeignete organisatorische und vertragliche Vorkehrungen sicher, dass dies in rechtlich zulässiger Weise möglich ist.

6.3. Der Auftraggeber ist verpflichtet, seinen Informationspflichten gegenüber Patienten, wie sie sich z.B. aus dem jeweiligen Krankenhausgesetz ergeben, umfassend nachzukommen.

6.4. Mitarbeiter von Dräger, die im Rahmen ihrer Aufgaben Einblick in Besondere Auftraggeberdaten erhalten können, werden bei Dräger regelmäßig zum ordnungsgemäßen Umgang mit personenbezogenen Daten geschult und zur Geheimhaltung von Patientendaten verpflichtet.

7. Weitere Vertragszwecke

7.1. Der Auftragnehmer hat das Recht, die von dieser Vereinbarung umfassten personenbezogenen Daten zu anonymisieren und vorher die für die Anonymisierung erforderlichen Verarbeitungsschritte durchzuführen. Der ursprüngliche Datenbestand ist von dieser Anonymisierung nicht betroffen.

7.2. Der Auftragnehmer 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.

7.3. Der Auftragnehmer 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 Auftragnehmer berücksichtigt auch in diesem Verarbeitungsprozess, dass vom Kunden gelöschte oder zur Löschung angewiesene Daten nicht mehr verarbeitet werden.

8. Kontrollen

8.1. 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 Auftraggeberdaten durch den Auftragnehmer 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 Auftragnehmer Technisch Organisatorische Maßnahmen sowie Testate von Wirtschaftsprüfern, der hauseigenen Revision oder Auditabteilung oder Auditberichte zur IT-Sicherheit und/oder Datenschutz vorlegen.

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

9. Haftung

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

10. Vertragslaufzeit, Vertragsende

10.1. 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.

10.2. 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.

11. Schlussbestimmungen

11.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichen“ im Sinne der EU-DSGVO liegen.

11.2. 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 Anlage im Übrigen nicht.

11.3. Der Auftragnehmer wird auch über das Ende des jeweiligen Vertrags hinaus Stillschweigen über die Auftraggeberdaten bewahren.

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

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

11.6. 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.

Der Hauptvertrag bleibt im Übrigen unberührt.