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

Präambel

Dieser Rahmenvertrag konkretisiert die datenschutzrechtlichen Verpflichtungen, die sich aus bestehenden oder künftigen Verträgen (nachfolgend einheitlich der "Hauptvertrag") zwischen dem Auftragsverarbeiter und dem Auftraggeber ergeben, soweit diese eine Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung (DS-GVO) zum Gegenstand haben.

Um die datenschutzgerechte Erbringung aller im Hauptvertrag vereinbarten Leistungen sicherzustellen, vereinbaren die Parteien, zusätzlich zu den in den Hauptverträgen bereits getroffenen Vereinbarungen zum Datenschutz, das Folgende:

1. Anwendungsbereich

1.1. Der Auftragsverarbeiter ist gemäß Hauptvertrag vom Auftraggeber mit der Erbringung von Leistungen 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 als Verantwortlichem dieser Daten oder aus der Sphäre des Auftraggebers stammen (nachfolgend „Auftraggeberdaten“), hat und diese verarbeiten wird.

1.2. Die in diesem Rahmenvertrag über die Auftragsverarbeitung enthaltenen Anforderungen gelten für alle Datenverarbeitungsvorgänge durch den Auftragsverarbeiter im Rahmen der Erbringung der vertraglich erforderlichen Leistungen. Er ergänzt und konkretisiert die Regelungen zum Datenschutz im Hauptvertrag, soweit der Auftragsverarbeiter nicht aufgrund von Pflichten aus dem Recht der Union oder der Mitgliedstaaten der EU zur Verarbeitung personenbezogener Daten verpflichtet ist (z. B. die Anforderungen an ein Qualitätssicherungsmanagement des Herstellers von Medizinprodukten gemäß Art. 83 der Medizinprodukteverordnung).

1.3. Dieser Rahmenvertrag ergänzt und konkretisiert die Regelungen zum Datenschutz im Hauptvertrag. Im Fall von Widersprüchen zu dem Hauptvertrag gehen die Regelungen dieses Rahmenvertrages vor. Sind aufgrund einer Folgebeauftragung Abweichungen von diesem Auftragsverarbeitungsvertrag erforderlich, so sind diese in einem Zusatz zu regeln, der Bestandteil dieses Rahmenvertrages wird.

2. Auftragsinhalt

Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus dem jeweiligen Hauptvertrag sowie ergänzend der **Anlage 1** zum vorliegenden Rahmenvertrag.

3. Pflichten des Auftragsverarbeiters

3.1. Der Auftragsverarbeiter beachtet bei der Verarbeitung von Auftraggeberdaten die am Sitz des Auftraggebers geltenden Datenschutzgesetze und in jedem Fall mindestens die Anforderungen der Datenschutzgrundverordnung (DS-GVO) sowie des Bundesdatenschutzgesetzes (BDSG), jeweils soweit diese für Leistungen des Auftragsverarbeiters gelten, insbesondere aber 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 gestaltet, dass sie den gesetzlichen Anforderungen des Datenschutzes gerecht wird.

3.2. Der Auftragsverarbeiter verarbeitet Auftraggeberdaten im Rahmen des Auftrags und entsprechend den mindestens in Textform erteilten Weisungen des Auftraggebers. Der Auftraggeber ist und bleibt als datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO.

3.3. Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach einer mindestens in Textform erteilten Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.4. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Vorschriften zum Datenschutz verstößt, weist der Auftragsverarbeiter den Auftraggeber mindestens in Textform darauf hin. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragsverarbeiter unterrichtet den Auftraggeber auf dem gleichen Weg bei schwerwiegenden Störungen des Betriebsablaufes, der Verletzung des Schutzes personenbezogener Daten oder anderen wesentlichen Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten. 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 diesem Rahmenvertrag betrifft.

3.5. Der Auftragsverarbeiter ist verpflichtet, bei der Verarbeitung von Auftraggeberdaten ausschließlich Personen einzusetzen, die zur Vertraulichkeit

verpflichtet wurden und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. 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. Soweit in Betracht kommt, dass das eingesetzte Personal Kenntnis von solchen Daten und Informationen erhält, die der ärztlichen Verschwiegenheitspflicht unterliegen, setzt der Auftragsverarbeiter nur solche Personen ein, die auf die Strafbarkeit der Offenbarung solcher Geheimnisse hingewiesen wurden.

3.6. Der Auftragsverarbeiter bestellt einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dieser Datenschutzbeauftragte ist unter der E-Mail-Adresse dataprivacy@draeger.com zu erreichen.

3.7. Nach Abschluss der Vertragsbeziehung wird der Auftragsverarbeiter alle personenbezogenen Auftraggeberdaten in Abstimmung mit dem Auftraggeber zurückgeben oder löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. Ziffer 10.3 gilt ergänzend.

3.8. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, und andere rechtlich zwingend vorzuhaltende Dokumente sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

3.9. Der Auftragsverarbeiter unterstützt den Auftraggeber in angemessenem Umfang bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den Artikeln 12 bis 22 der DS-GVO genannten Rechte der betroffenen Person nachzukommen und bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen 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 Feststellung von relevanten Verletzungsereignissen ermöglichen. Eine Dokumentation der technischen und organisatorischen Maßnahmen des Auftraggebers ist diesem Vertrag als **Anlage 2** beigefügt.
- die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
- die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem

Zusammenhang sämtliche vorliegenden relevanten Informationen zeitnah zur Verfügung zu stellen.

- die Unterstützung des Auftraggebers bei einer Datenschutz-Folgenabschätzung.
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

3.10. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde informieren, soweit diese sich konkret auf die Auftraggeberdaten beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Verarbeitung von Auftraggeberdaten beim Auftragsverarbeiter ermittelt.

3.11. 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.

3.12. 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. Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten.

3.13. Der Auftragsverarbeiter führt ein Verzeichnis über alle Verarbeitungstätigkeiten, bei denen personenbezogene Daten verarbeitet werden. Er stellt dieses Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

4. Unterauftragsverarbeiter

4.1. Leistungen von Unterauftragsverarbeitern sind Leistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z. B. als Post-, Transport- oder Reinigungsdienstleistungen in Anspruch nimmt. Der Auftragsverarbeiter ist gleichwohl verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Auftraggeberdaten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

4.2. Der Auftraggeber stimmt zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter hinzuzieht. Vor Hinzuziehung oder Ersetzung der

Unterauftragsverarbeiter informiert der Auftragsverarbeiter den Auftraggeber und gibt diesem Gelegenheit, innerhalb angemessener Frist (zumindest 28 Tage) bei Vorliegen wichtiger Gründe zu widersprechen. Ein Widerspruch berechtigt den Auftragsverarbeiter zur sofortigen Kündigung dieses Vertrags sowie des zugehörigen Hauptvertrags. Eine Auflistung bereits bei Unterzeichnung dieses Vertrags eingesetzter Unterauftragsverarbeiter findet sich in der **Anlage 1** im Rahmen der Darstellung der unterschiedlichen Leistungsmodule**.** Der Einsatz der in **Anlage 1** aufgezählten Unterauftragsverarbeiter gilt hiermit als genehmigt.

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

4.4. Erbringt der Unterauftragsbearbeiter die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch geeignete Maßnahmen nach Art. 44 ff. DS-GVO sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 4.1 Abs. 1 Satz 2 eingesetzt werden sollen.

5. Pflichten des Auftraggebers

5.1. Der Auftraggeber beurteilt die Zulässigkeit der Verarbeitung von Auftraggeberdaten durch den Auftragsverarbeiter im Rahmen des Hauptvertrags 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 Auftragsverarbeiter unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten unterrichten, insbesondere bei der Prüfung der Ergebnisse der Auftragsverarbeitung.

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 Auftragsverarbeiter unterstützt den Auftraggeber bei dieser Pflicht durch Zurverfügungstellung der erforderlichen Informationen.

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 die Auftraggeberdaten selbst als Auftragsverarbeiter für einen Dritten verarbeitet und die Tätigkeit des Auftragsverarbeiters daher eine Unterauftragsverarbeitung darstellt, stellt der Auftraggeber sicher, dass der Dritte Verantwortlicher im Sinne der DS-GVO bleibt und die ihm nach der DS-GVO zustehenden Rechte hat. Der Auftraggeber beauftragt den Auftragsverarbeiter in diesen Fällen nur, wenn er zuvor die Genehmigung des Dritten eingeholt hat. Er

stellt außerdem sicher, dass dem Auftragsverarbeiter 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 treffen, 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 Auftragsverarbeiter verantwortlich ist.

5.6. Allgemeine Weisungen des Auftraggebers für den Umgang mit Auftraggeberdaten bedürfen mindestens der Textform. Mündliche Weisungen des Auftraggebers im Einzelfall dürfen nur durch hierzu autorisierte und dem Auftragsverarbeiter im Vorfeld ausdrücklich benannte Personen erfolgen. Mündliche Weisungen sind durch den Auftraggeber mindestens in Textform zu bestätigen.

5.7. Der Auftraggeber führt ein Verzeichnis zu allen Kategorien von durch ihn durchgeführten Verarbeitungstätigkeiten.

6. Besonders geschützte Daten

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, sowie für Daten, die unter das Berufsgeheimnis i. S. d. § 203 StGB fallen können („Besondere Auftraggeberdaten“).

6.2. Der Auftraggeber wird dafür Sorge tragen, dass der Auftragsverarbeiter bei der Durchführung der vertraglichen Leistungen keinen Zugriff auf besondere Auftraggeberdaten hat, soweit dies nicht zur Leistungserbringung zwingend erforderlich ist. 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 Mitarbeitern und Kunden, wie sie sich z. B. aus den lokalen Gesetzen ergeben, umfassend nachzukommen.

6.4. Der Auftragsverarbeiter verpflichtet sich, über besondere Auftraggeberdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

6.5. Dem Auftragsverarbeiter ist bekannt, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S.1 StGB strafbar machen. Der Auftragsverarbeiter stellt sicher, dass alle Beschäftigten, die im Rahmen der

Auftragserfüllung eingesetzt werden und dabei mit besonderen Auftraggeberdaten in Kontakt kommen, über die Strafbarkeit gem. § 203 StGB informiert und zur Geheimhaltung der ihnen bei der Ausübung oder Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse verpflichtet 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 Auftraggeberdaten durch den Auftragsverarbeiter zu überzeugen.

7.2. 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 – Technische und Organisatorische Maßnahmen** oder Testate von Wirtschaftsprüfern, der hauseigenen Revision oder Auditabteilung oder Auditberichte zur IT-Sicherheit und/oder Datenschutz vorlegen.

7.3. 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

Auftraggeber und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Eventuelle Haftungsbeschränkungen des Hauptvertrages gelten entsprechend.

9. Vertragslaufzeit, Vertragsende und bestehende Verträge

9.1. Dieser Rahmenvertrag wird auf unbestimmte Zeit geschlossen. Mit Beendigung des Hauptvertrages und aller hieraus resultierenden Einzelbeauftragungen endet dieser Rahmenvertrag automatisch, ohne dass es einer gesonderten Kündigung bedarf.

9.2. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

9.3. Soweit zwischen den Parteien bereits Auftragsverarbeitungsverträge bestehen, werden diese durch den vorliegenden Rahmenvertrag ersetzt.

10. Schlussbestimmungen

10.1. Sollten die Daten des Auftraggebers 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 unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang relevanten Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als datenschutzrechtlich Verantwortlichem im Sinne der DS-GVO liegen.

10.2. Bei etwaigen Widersprüchen gehen Regelungen dieses Rahmenvertrages den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Rahmenvertrages unwirksam sein, so berührt dies die Wirksamkeit des Rahmenvertrags im Übrigen nicht.

10.3. Mit Ende des Hauptvertrages gibt der Auftragsverarbeiter die personenbezogenen Auftraggeberdaten samt Datenträger heraus oder vernichtet sie auf Wunsch nach dem Stand der Technik unwiederbringlich. Der Auftragsverarbeiter ist auch dann zur Vernichtung berechtigt, wenn die Auftraggeberdaten weder abgerufen 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 dieser Rahmenvertrag bis zu deren Vernichtung fort gilt.

10.4. Es gibt keine mündlichen Nebenabreden. Änderungen und Ergänzungen dieses Rahmenvertrags bedürfen der Schriftform (elektronische Form – etwa via elektronischer Signatur – genügt). 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.

- **Anlage 1 - Gegenstand, Art und Zweck der Datenverarbeitung, Unterauftragsverarbeiter**

- **Anlage 2 – Technische und organisatorische Maßnahmen**

Anlage 1: Gegenstand, Art und Zweck der Datenverarbeitung, Unterauftragsverarbeiter

Gegenstand, Art und Zweck der Datenverarbeitung sind abhängig von den durch den Auftragsverarbeiter nach Maßgabe des Hauptvertrags geschuldeten Leistungen. Die nachfolgend aufgeführten Module und hiermit verbundenen Verarbeitungstätigkeiten finden folglich jeweils nur insoweit Anwendung, als sie vom Auftraggeber beauftragt worden sind.

a) Grundlagen

Das Dräger Smart Rescue (DSRS) ist ein digitales Einsatzinformationssystem mit Mandantenverwaltung für Behörden mit öffentlichen Sicherheitsaufgaben. Dies beinhaltet die Bereitstellung von Informationen zur Alarmmeldung, von Informationen zum Einsatzort, z. B. in Form von Kartenansichten, Gebäudedaten etc. zur Bereitstellung von ergänzenden Ressourcen, z. B. Kfz-Rettungskarten oder Gefahrgutinformationen etc..

b) Datenkategorien:

Gegenstand der Verarbeitung können abhängig von der Nutzung folgende Kategorien personenbezogener Daten sein:

- Einsatzinformationen (z. B. Verfügbarkeiten, Einsatzort, Einsatzinhalt)
- Kommunikationsdaten (z. B. zur Einsatzabstimmung)
- Beschäftigtendaten (z. B. Stammdaten von Beschäftigten wie Name, Kontaktdaten wie etwa E-Mail-Adresse oder Telefonnummer)

c) Betroffenenkategorien:

Von der Verarbeitung betroffen sind die folgenden Personengruppen:

- Beschäftigte oder Einsatzkräfte
- sonstige Betroffene wie etwa den Einsatz Meldende, Zeugen, Geschädigte

d) Unterauftragsverarbeiter:

- Für das Hosting mittels EC2 (Elastic Compute Cloud) und Speicherung von großen Daten in S3 wird Amazon Web Services Inc. eingesetzt. Die eingesetzten Server befinden sich in Deutschland in einem C5 zertifizierten Rechenzentrum (eu-central-1).
- Bei Kunden mit Alarmeingang via Emailanbindung wird für SES (Simple Email Service) zum Empfangen von Emails und SNS (Simple Notification Service) zur Informationsweitergabe bei eingehenden Emails Amazon Webservices eu-west-1 in Irland genutzt
- Google Ireland Ltd, Dublin stellt die Kartennutzung, das Geocoding sowie die Push-Funktionalitäten bereit.

- Dienste von Okta Inc. werden zur Registrierung und Verwaltung von Benutzeranmeldungen genutzt
- Dienste von Sentry Inc. werden zum Monitoring und zur Fehleranalyse verwendet
- Dienste von Drägerwerk AG & Co. KGaA werden zur Bereitstellung und zum Support genutzt

Im Übrigen gelten die Ausführungen des Rahmenvertrags für die Auftragsverarbeitung.

Anlage 2: Technische und Organisatorische Maßnahmen

Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten gemäß Artikel 28 und 32 DSGVO sowie zum Schutz von Geschäftsgeheimnissen

Inhalt

1. Vertraulichkeit der Systeme und Dienste
- 1.1. Zutrittskontrolle
- 1.2. Zugangskontrolle
- 1.3. Zugriffskontrolle
- 1.4. Pseudonymisierung und Verschlüsselung

2. Integrität der Systeme und Dienste
- 2.1. Eingabekontrolle
- 2.2. Weitergabekontrolle
- 2.3. Trennungskontrolle

3. Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- 3.1. Verfügbarkeitskontrolle
- 3.2. Belastbarkeit
- 3.3. Wiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- 4.1. Datenschutz- und Sicherheitsmaßnahmen
- 4.2. Incident-Response-Management
- 4.3. Auftragskontrolle

1. Vertraulichkeit der Systeme und Dienste

1.1. 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 zu den Betriebsstätten bzw. Niederlassungen über folgende Maßnahmen:

a) berechtigungsgesteuerte Zutrittsausweise (Kartenlesegeräte an den Haupt- und Nebentoren des Firmengeländes) und/oder manuelle Schließsysteme mit Schlüsselregelung und/oder Codesperre
b) Besuchermanagement (Empfang, Protokoll, Begleitung, visuelle Kennzeichnung)
c) Alarmanlagen und Gebäudeüberwachung
d) Sicherung der Werksgelände in Lübeck durch sorgfältig ausgewähltes Wachpersonal
e) sorgfältige Auswahl der Reinigungsdienste

1.2. Zugangskontrolle

Zugangskontrolle fasst jene Maßnahmen zusammen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt oder auf diese unberechtigt zugegriffen werden können.

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

a) Login mit User-ID und Passwort
b) Bildschirmsperre mit Passwortaktivierung
c) Fernwartung erfolgt nur über ein Portalsystem mit eigenen Zugriffscodes und einem dedizierten Berechtigungskonzept oder über eine individuelle Sitzungsfreigabe durch den Nutzer.
d) Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort. Die Passwortkomplexität und Änderungszyklen richten sich nach dem Stand der Technik, entsprechend den Vorgaben des BSI.
e) Mehrfaktor-Authentifizierung
f) zentrale Vorgaben zur Löschung/Vernichtung
g) zentral gesteuerte Datenschutz- und Informationssicherheitsbestimmungen und dazu gehöriges Schulungskonzept mit verpflichtenden Schulungen
h) Durchsetzung der Policies durch Endgerätemanagement (MDM, MEM)
i) funktionelle Zuordnung der Datenendgeräte zu Nutzern
j) ein dediziertes Rollen-/ Rechtekonzept für jedes Gerät

1.3. 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 und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die relevanten IT-Systeme, mit denen 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.

Speichermedien des Auftraggebers, die außer Betrieb genommen werden, werden einem kontrollierten und dokumentierten Zerstörungsprozess zugeführt.

Durch den Auftragsverarbeiter zum Zwecke der Leistungserbringung erstellte Kopien in Papierform werden – sofern auf Dräger Werksgeländen – mit Aktenvernichtern oder in verschlossenen Datenschutzcontainer entsorgt, die in einem datenschutzrechtlich freigegebenen Verfahren von einem spezialisierten Dienstleister entsorgt werden, mit dem ein Auftragsverarbeitungsvertrag besteht. Sollten Kopien in Papierform beim Kunden entsorgt werden, werden die dortigen Vorgaben bzw. Prozesse befolgt.

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 Auftraggeber.

Diese Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

Alle Informationen und Dokumente bei Dräger werden anhand von Klassifizierungen der Vertraulichkeit eingestuft. Auf Grundlage dieser Klassifizierungen (public/internal/confidential/strictly confidential) sind technische und organisatorische Schutzmaßnahmen definiert.

1.4. Pseudonymisierung und Verschlüsselung

Die Verarbeitung erfolgt nach Möglichkeit in einer Weise, dass die Daten ohne Hinzuziehung weiterer Informationen nicht mehr einer betroffenen Person zugeordnet werden können (pseudonymisiert). Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen (bspw. Verschlüsselung).

Dräger nutzt bei seinen elektronischen Verfahren in der Regel auch möglichst umfassende Verschlüsselung in Verbindung mit Berechtigungssystemen. Dadurch wird gesteuert, wer Zugriff auf die zu schützenden Daten hat. Es gibt dabei

kontextspezifische Ansatzpunkte zur Verschlüsselung und Schlüsselmanagement, die das „need to know“ Prinzip befolgen. Für die Wahl der richtigen Technologie und Umfang der Verschlüsselung ist dabei sowohl die Sicherheit aber auch Funktionalität des Produktes ausschlaggebend.

Folgende konkrete Maßnahmen sind etabliert:

a) Festplatten in Arbeitsrechnern werden mit BitLocker verschlüsselt
b) USB-Sticks werden Hardware-verschlüsselt (AES 256 bit) zur Verfügung gestellt

Es bestehen interne Vorgaben, personenbezogene Daten, die für Kunden verarbeitet werden, nach den Prinzipien von „Privacy by Design“ zu verarbeiten (Datenminimierung, Datentrennung, Speicherbegrenzung, technische Schutzmaßnahmen, Pseudonymisierung und Anonymisierung).

2. Integrität der Systeme und Dienste

2.1. 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.

Folgende Maßnahmen werden dazu stets bei Dräger umgesetzt:

a) Protokollierung der Eingabe, Änderung und Löschung von Datensätzen
b) Nachvollziehbarkeit durch eindeutige Benutzernamen
c) Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten
d) Monitoring von Unregelmäßigkeiten, auch in den Anmeldeversuchen, werden über ein automatisiertes SIEM (Security Incident Event Management) überwacht, das von einem dedizierten SOC (Service Operation Center) betrieben und ausgewertet wird

2.2. 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:

a) Virenschutz auf allen von Dräger zur Verfügung gestellten Endgeräten
b) Netzwerksegmentierung
c) Firewalls an den Netzwerkgrenzen und Netzwerksegmenten
d) Einsatz von Spamfilter mit kontinuierlichen Aktualisierungen
e) VPN (Virtual Private Networks) ins Dräger Global Network
f) Content Filter / Proxys und DMZ (Demilitarisierte Zonen)
g) IPS /IDS (Intrusion Detection /Prevention Systems) an den Internet Outbreaks
h) Verschlüsselung von E-Mails (über S/MIME)
i) Prozesse zur elektronischen Signatur etabliert
j) Patch- und Updatemanagement für die Endgeräte

2.3. 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:

a) mandantenfähige Anwendungen und logische Mandantentrennung
b) funktionale Trennung in Produktiv-, Test- und Entwicklungsumgebung
c) Steuerung über Berechtigungskonzept
d) Festlegung von Datenbankzugriffsrechten

3. Verfügbarkeit und Belastbarkeit der Systeme und Dienste

3.1. Verfügbarkeitskontrolle

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

Bei Dräger werden im Rahmen von Service Aktivitäten die Daten des Auftraggebers nur innerhalb der Infrastruktur des Auftraggebers verarbeitet. Ein Ausfallen der Systeme bei Dräger hätte für diese Fälle daher schlimmstenfalls nur zur Folge, dass die anhängige Wartung verschoben werden müsste.

Davon unabhängig sind folgende Maßnahmen standardmäßig für die Bereitstellung von Infrastruktur bei Dräger implementiert:

a) Feuer- und Rauchmeldeanlagen
b) wasserfreie Feuerlöschsysteme in Serverräumen
c) Klimatisierung und Überwachung der Serverräume
d) USV (Unterbrechungsfreie Stromversorgung) mittels Diesel-Generatoren
e) NAS Speichersysteme, die RAID Systeme / Festplattenspiegelung beinhalten
f) aktive Überwachung zentraler Systeme und Alarming mit Wiederherstellungsprozessen
g) Backup Verfahren mit Anwendungsspezifischen Zyklen
   Das im Rahmen von Service Aktivitäten eingesetzte Fernwartungssystem wird im Rechenzentrum eines Dienstleisters von Dräger betrieben, der ISO 27001 zertifiziert ist. Mittels SLAs wird sichergestellt, dass die Systeme ausfallsicher betrieben werden.

3.2. Belastbarkeit

Belastbarkeit wird als eine Kombination von Robustheit und Resilienz verstanden. Dabei beinhaltet Robustheit eine Härtung der eingesetzten Komponenten entsprechend dem Risikoniveau und Resilienz die Maßnahmen, die getroffen werden, um auch auf unerwartete Störungen reagieren zu können.

Die bei Dräger eingesetzten IT-Systeme werden gemäß ihres Einsatzes gehärtet sowie regelmäßig auf Schwächen geprüft sowie Penetrationstests von externen Anbietern durchgeführt. Identifizierte Sicherheitslücken werden bewertet und umgehend behoben.

Selbst entwickelte Software wird zusätzlich regelmäßig von einem Risikomanagementsystem auf die OWASP10 Kriterien geprüft.

Um auf unvorhergesehene Zwischenfälle reagieren zu können, ist bei Dräger in der IT ein Security Incident Response Management Prozess etabliert, der für besonders kritische Fälle auch die Einberufung eines CERT (Computer Emergency Response Team) vorsieht.

- Vulnerability Management
- Forensic systems
- Cyber Threat Intellicence

3.3. Wiederherstellbarkeit

Im Kontext von Remote Service und kontinuierlichem Monitoring ist gewährleistet, dass die Verfügbarkeit der Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unmittelbar wiederhergestellt werden kann. Im Falle einer Fernwartung hat ein Zwischenfall im Rahmen des Zugriffs keinen Einfluss auf die Verfügbarkeit.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz- und Sicherheitsmaßnahmen

Das bei Dräger implementierte Datenschutzmanagementsystem besteht aus Richtlinien, Schulungen und einem Tool-gestützten Verzeichnis von Verarbeitungstätigkeiten. Das Verzeichnis wird jährlich aktualisiert. Zur Meldung neuer oder veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten sind (im IMS dokumentierte) Prozesse etabliert und geschult. Bei Bedarf wird eine Datenschutz-Folgenabschätzung durchgeführt, um eine sichere Verarbeitung zu wahren. Die Kontrolle erfolgt stichprobenhaft durch Datenschutzaudits.

Zur Wahrung der datenschutzfreundlichen Voreinstellungen werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Die Umsetzung wird überdies durch Vorgaben und Merkblätter sichergestellt. Darüber hinaus ist eine einfache Ausübung des Widerrufsrechts der Betroffenen durch technische Maßnahmen implementiert.

Für die eingesetzten IT-Systeme werden die umgesetzten Maßnahmen in Sicherheitskonzepten festgehalten und hinsichtlich der Wirksamkeit der technischen Maßnahmen regelmäßig überprüft.

Die Mitarbeiter werden regelmäßig für den sicheren Umgang mit personenbezogenen Daten sensibilisiert und geschult sowie zur Vertraulichkeit verpflichtet. Darüber hinaus existiert eine zentrale Dokumentation der Verfahrensweisen und Regelungen zum Datenschutz bei Dräger.

4.2. Incident-Response-Management

Zum Incident-Response-Management werden die Maßnahmen genannt, die zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen dienen.

Es existiert ein im Risikomanagement und IT-Management verankerter Prozess zur Vorbereitung und zur Identifizierung und Behebung von Sicherheitsverletzungen und Systemstörungen. Außerdem gibt es einen Prozess zur Meldung von Sicherheitsvorfällen (auch im Hinblick auf die Meldepflicht an die Aufsichtsbehörde). Hierbei ist auch die Einbindung des Datenschutzbeauftragten geregelt. Jegliche Sicherheitsvorfälle werden zentral dokumentiert und abgelegt. Durch einen ausführlichen End Of Day Report werden die täglich getroffenen Maßnahmen zur Risikoprävention eines Sicherheitsvorfalls festgehalten.

4.3. 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 Auftragsverarbeiter („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 Dienstleistern erfolgt, neben den gesetzlichen Anforderungen, auf der Basis der bei Dräger gültigen Standards.

Weiter ist eine Information an den Bereich Datenschutz sowie eine Kontrolle des Auftragsverarbeiters im Hinblick auf die von ihm getroffenen technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit vorzunehmen. Dräger verpflichtet seine Auftragsverarbeiter, 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 Auftragsverarbeiter zu erteilen und die Einhaltung der Vorgaben durch Kontrollen sicherstellen. Auch der Einsatz weiterer Untersubunternehmer ist nur nach vorheriger Mitteilung an Dräger möglich.

Die eingesetzten Auftragsverarbeiter wurden durch einen Vertrag zur Auftragsverarbeitung (AVV) zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet. Bei Transfer der Daten in ein Drittland werden dem Subunternehmer zudem die EU-Standardvertragsklauseln auferlegt, sofern nicht durch einen Angemessenheitsbeschluss ausgenommen.

Die relevanten Auftragsverarbeiter sind:

a) Dienstleister zum Betrieb und Management der Client Rechner sowie der darauf genutzten Software
b) Dienstleister zum Betrieb und Management des Netzes und der Netzzugänge
c) Dienstleister zur Entsorgung von papierbasierten Dokumenten und elektronischen Speichermedien