Technische und Organisatorische Maßnahmen (Dräger Gruppe)

Diese technischen und organisatorischen Maßnahmen der Dräger Gruppe zum Schutz personenbezogener Daten gemäß den Artikeln 28 und 32 DS-GVO und Informationen zum Schutz von Geschäftsgeheimnissen, unterliegen unter der Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und Zwecke, sowie der Eintrittswahrscheinlichkeit von und Schwere der Risiken, einer ständigen Weiterentwicklung und können in der jeweils aktuellen Version unter www.draeger.com/dpa abgerufen werden.

1. Cyberhygiene

Cyberhygiene umfasst die Anwendung grundlegender Verfahren und Herangehensweisen, welche allgemein zu einer Verbesserung des Cybersicherheitsniveaus einer Einrichtung führen.

1.1. Patchmanagement
Auf den von Dräger verwalteten Endgeräten wird ein zentralisiertes Patch- und Updatemanagement durchgeführt. Für Netzelemente und Sever-Infrastruktur gibt es dezidierte Vorgaben und regelmäßige Kontrollen zum Patch- und Updatemanagement. Bei entdeckten Sicherheitslücken wird Software in Abhängigkeit der Kritikalität aktualisiert oder, wenn nicht anders möglich, das betroffene System isoliert.

1.2. Regelungen für sichere Passwörter
Die Dräger Passwortrichtline gibt vor, wie sichere Passwörter nach aktuellem Stand der Technik zu gestalten sind, und wie IT-Systeme dies implementieren müssen.

1.3. Verwaltung von Geräten und Gerätekonfigurationen
Ein Management zur Verwaltung und Konfiguration von den verschiedenen eingesetzten Endgeräten wird bei Dräger zentral betrieben.

1.4. Identitäts- und Zugriffsmanagement
Ein für die Dräger Gruppe betriebenes Identitätsmanagement steuert das Zugriffsmanagement auf Endgeräten und für Systemaccounts.

1.5. Netzwerksegmentierung
Netzwerke werden bei Dräger nach Funktionen getrennt und ermöglichen so jeweils kontextspezifische Schutzmaßnahmen.

1.6. Backup- und Sicherungskonzepte für Daten
Für Systeme mit schützenswerter Information sind bei Dräger Backup- und Sicherheitskonzepte vorhanden, die fallspezifisch gewähren, dass die relevante Information nicht verloren geht und Systeme in jeweils angemessener Zeit neu aufgesetzt werden können.

1.7. Schutz vor Schadsoftware
Auf den Rechnern, Servern und im Netz von Dräger laufen leistungsfähige Programme zur Erkennung und Beseitigung von Schadsoftware. Diese Programme und Ihre Erkennungsmuster werden kontinuierlich aktuell gehalten.

2. Vertraulichkeit der Systeme und Dienste

2.1. 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:

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

2.2. 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:

- Login mit User-ID und Passwort
- Bildschirmsperre mit Passwortaktivierung
- Fernwartung erfolgt nur über ein Portalsystem mit eigenen Zugriffscodes und einem dedizierten Berechtigungskonzept oder über eine individuelle Sitzungsfreigabe durch den Nutzer.
- 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.
- Mehrfaktor-Authentifizierung
- zentrale Vorgaben zur Löschung/Vernichtung
- zentral gesteuerte Datenschutz- und Informationssicherheitsbestimmungen und dazu gehöriges Schulungskonzept mit verpflichtenden Schulungen
- Durchsetzung der Policies durch Endgerätemanagement (MDM, MEM)
- funktionelle Zuordnung der Datenendgeräte zu Nutzern
- ein dediziertes Rollen-/ Rechtekonzept für jedes Gerät

2.3. 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.

2.4. 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:
- Festplatten in Arbeitsrechnern werden mit BitLocker verschlüsselt
- 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).

3. Integrität der Systeme und Dienste

3.1. 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:
- Protokollierung der Eingabe, Änderung und Löschung von Datensätzen
- Nachvollziehbarkeit durch eindeutige Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten
- Monitoring von Unregelmäßigkeiten, auch in den Anmeldeversuchen, werden über ein automatisiertes Security Incident Event Management (SIEM) überwacht, das von einem dedizierten Service Operation Center (SOC) betrieben und ausgewertet wird

3.2. 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:

- Virenschutz auf allen von Dräger zur Verfügung gestellten Endgeräten
- Netzwerksegmentierung
- Firewalls an den Netzwerkgrenzen und Netzwerksegmenten
- Einsatz von Spamfilter mit kontinuierlichen Aktualisierungen
- VPN (Virtual Private Networks) ins Dräger Global Network
- Content Filter / Proxys und DMZ (Demilitarisierte Zonen)
- Verschlüsselung von E-Mails
- Prozesse zur elektronischen Signatur etabliert
- Patch- und Updatemanagement für die Endgeräte

3.3. 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:

- mandantenfähige Anwendungen und logische Mandantentrennung
- funktionale Trennung in Produktiv-, Test- und Entwicklungsumgebung
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankzugriffsrechten

4. Verfügbarkeit und Belastbarkeit der Systeme und Dienste

4.1. Verfügbarkeitskontrolle

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

Bei Dräger werden folgende Maßnahmen standardmäßig für die Bereitstellung von Infrastruktur bei Dräger implementiert:

- Feuer- und Rauchmeldeanlagen
- wasserfreie Feuerlöschsysteme in Serverräumen
- Klimatisierung und Überwachung der Serverräume
- USV (Unterbrechungsfreie Stromversorgung) mittels Diesel-Generatoren
- NAS Speichersysteme, die RAID Systeme / Festplattenspiegelung beinhalten
- aktive Überwachung zentraler Systeme und Alarming mit Wiederherstellungsprozessen
- Backup Verfahren mit Anwendungsspezifischen Zyklen

4.2. 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 ihrem Einsatz gehärtet, auf Schwächen geprüft sowie Penetrationstests von externen Anbietern durchgeführt.

Identifizierte Sicherheitslücken werden bewertet und in Abhängigkeit der Kritikalität behandelt.

Selbst entwickelte Software wird zusätzlich regelmäßig von einem Risikomanagementsystem unter anderem 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.

Die Dräger IT betriebt ein kontinuierliches, toolgestütztes Vulnerability Management, das für die kontinuierliche Identifikation und Behebung von Sicherheitslücken sorgt. Dazu gehören regelmäßige Scans und ein klar definierter Patch-Prozess, die eine Minimierung von Risiken gewährleisten.

Dräger nutzt aktuelle Cyber Threat Intelligence, um Bedrohungen frühzeitig zu erkennen und proaktiv zu reagieren. Informationen aus vertrauenswürdigen Quellen fließen in die Sicherheitsstrategie ein und stärken die Abwehrmaßnahmen.

Über speziell bereitgestellte forensische Systeme können mögliche Sicherheitsvorfälle lückenlos analysiert und Beweise gerichtsfest gesichert werden. Automatisierte Protokollierung und zentrale Datenhaltung ermöglichen dabei eine schnelle und präzise Untersuchung.

4.3. 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.

5. Fernwartung von Medizinprodukten

Fernwartung von Medizinprodukten und/oder im medizinischen Kontext, umfasst die Maßnahmen im Bereich unseres Leistungsangebotes gegenüber Kunden der Medizintechnik, die gewährleisten, dass der räumlich getrennte Zugriff auf IT-Systeme zu Wartungs- und Reparaturzwecken geschützt vor dem Zugriff Unberechtigter erfolgen kann. Dies erfolgt nur in den Fällen, wenn dies mit dem Auftraggeber vertraglich vereinbart wurde und die vom Auftragsverarbeiter bereitgestellten technischen Lösungen verwendet werden. Für die vom Auftragsverarbeiter bereitgestellten Fernwartungslösungen sind die unter dem Abschnitt Zugangsart, Verbindungsaufbau und Sicherheitsmaßnahmen, angeführten technischen und organisatorischen Voraussetzungen getroffen.

Wird in besonderen Ausnahmefällen – die gesondert zwischen dem Auftraggeber und Auftragsverarbeiter vereinbart werden – stattdessen eine vom Auftraggeber bereitgestellte technische Lösung zur Fernwartung genutzt, gewährleistet allein der Auftraggeber, in der Rolle als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO, insoweit insbesondere die Einhaltung eines angemessenen Sicherheitsniveaus nach Art. 24, 25 und 32 DS-GVO.

5.1. Zugangsart

Grundsätzlich wird das Auftraggebernetz über eine gesicherte Verbindung zu dedizierten Systemen des Auftraggebers erreicht, die nach dem Aufbau der Verbindung entweder E2E-verschlüsselt ist, oder jeweils Punkt zu Punkt verschlüsselt über einen

Vermittlungsserver geführt wird, der von sorgfältig ausgewählten und geprüften Dienstleistern für bestimmte, wählbare Verschlüsselungsformen bereitgestellt wird. Die Verschlüsselung wird je nach Stand der aktuellen Technik auch für besonders kritische Daten ausreichend sicher gewählt.
Nach Wunsch des Auftraggebers ist eine Beschränkung des Zugriffes z. B. auf die Tageszeit und den Teilnehmerkreis möglich. Dort wo 24/7 Supportverträge bestehen, ist ein 24/7 Zugriff auf die Einwahlknoten mandatorisch.
Die Fernwartung wird fast ausschließlich auf Serversystemen durchgeführt; der Endanwender des Auftraggebers arbeitet an abgesetzten Arbeitsstationen, auf die nur im absoluten Ausnahmefall in Abstimmung mit dem Personal vor Ort zugegriffen wird.

5.2. Verbindungsaufbau
Um den Kontakt zwischen dem Fernwartungsrechner und dem Gateway im Kundennetzwerk herzustellen, wird ein gesicherter Vermittlungsserver eines Portalsystems per HTTPS aufgerufen, der den Kontakt zwischen den betreffenden Endgeräten herstellt, damit ein verschlüsselter Tunnel etabliert werden kann. Schematisch wird der Verbindungsaufbau wie folgt realisiert:

Fernwartungsrechner -> Vermittlungsserver -> zu wartendes System des Auftraggebers. Der Dräger Fernwartungsrechner verbindet sich zum Vermittlungsserver. Erst nach einer erfolgreichen Authentifizierung kann der benannte Dräger Service Mitarbeitende nur auf die ihm zugewiesenen Geräte des Auftraggebers zugreifen und zu diesen eine Verbindung aufrufen.

5.3. Sicherheitsmaßnahmen
Ferner ist sichergestellt, dass
- die Remote-Verwaltungssoftware sich bei Verbindungsabbruch beendet;
- der Auftraggeber jederzeit die Fernwartung abbrechen kann;
- eine Protokollierung des Zugriffs stattfindet;

6. Auftragskontrolle

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

6.1. 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.

6.2. 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.

6.3. 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:

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

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1. 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.

7.2. 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.