ottobock.

Policy.
Data Privacy Management System.

Version 1.0 / März 2024

Vorwort.

Liebe Kolleginnen und Kollegen,

der Schutz ihrer personenbezogenen Daten und der personenbezogenen Daten von allen, mit denen wir zu tun haben, insbesondere unserer Patienten, ist der Ottobock ein grundlegendes Anliegen. In Deutschland sowie in der Europäischen Union unterliegen wir den Bestimmungen der Datenschutzgrundverordnung (DSGVO) sowie dem Bundesdatenschutzgesetz (BDSG) und im Vereinten Königreich dem gleichlautenden UK Data Protection Act 2018 (gemeinsam auch GDPR), welche ein umfassendes Datenschutzrecht darstellen, das auf den Schutz von personenbezogenen Daten und den Schutz der Daten von natürlichen Personen in der EU, dem Europäischen Wirtschaftsraum sowie im Vereinten Königreich zielt. Auch außerhalb der EU wird das Datenschutzrecht weiter modernisiert und gewinnt zunehmend an Bedeutung.
Ottobock entwickelt sich immer weiter zu einem datengetriebenen Unternehmen. Strategisch werden wir personenbezogene Daten zunehmend nutzen, um die Produkte und Services der Ottobock und die Versorgung der Patienten zu verbessern. Dazu müssen wir gewährleisten, dass unsere Datenschutz-Organisation den neuen Anforderungen entspricht.

Mit dieser Policy möchten wir daher die organisatorische Verantwortlichkeit entsprechend anpassen, um sicherstellen zu können, dass wir den zukünftigen Herausforderungen gerecht werden können.

Inhalt.

Geltungsbereich

Diese Policy gilt für alle Mitarbeiter und Organmitglieder (Aufsichtsorgane, geschäftsführende Direktoren, Mitarbeiter mit und ohne Führungsverantwortung) der Ottobock SE & Co. KgaA (im Folgenden: Ottobock).

Zielsetzung des Dokuments

Die Policy Data Privacy Management System (Policy DPMS) geht zum einen auf die Bedeutung von Datenschutz und Notwendigkeit eines Data Privacy Management Systems (DPMS) im Allgemeinen ein und gibt zum anderen einen Überblick über das DPMS von Ottobock. Zudem ist die Ausgestaltung der einzelnen Elemente im Detail beschrieben, welche den aufbau- sowie ablauforganisatorischen Rahmen für das DPMS bilden.

Die Policy soll einen Überblick für die mit dem DPMS verbundenen Aufgaben und Verantwortlichkeiten vermitteln. Sie soll zusammen dazu beitragen, dass entsprechende Regelungen, Prozesse und Verfahren zur Minimierung von Datenschutz-Risiken eingeführt, beschrieben und eingehalten werden. Sie soll die Grundlage für ein gruppenweites DPMS darstellen.

Bereichsbezeichnung „Cyber Security“ und „Fachbereich Data Privacy“

Die organisatorische Einheit bei Ottobock, die für die Entwicklung und Implementierung des DPMS zuständig ist, ist der Fachbereich „Cyber Security“. Mit der Benennung des Fachbereichs im Zusammenhang mit in dieser Policy beschriebenen Aufgaben und/oder Verantwortlichkeiten ist grundsätzlich derjenige organisatorische Teil des Fachbereichs gemeint, der sich mit Data Privacy Management-Aufgaben befasst. Somit wird im Folgenden der Fachbereich als „Fachbereich Data Privacy“ bezeichnet, um eine bessere Lesbarkeit zu erreichen und Fehldeutungen im Zusammenhang mit Aufgaben und/oder Verantwortlichkeiten zu vermeiden.

Gleichstellungshinweis

Zur besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher, weiblicher und diverser Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

A. DATENSCHUTZ UND DATA PRIVACY MANAGEMENT SYSTEM

1. Datenschutz-Compliance – was bedeutet das für Ottobock?

Unter „Datenschutz-Compliance“[1] wird bei Ottobock die Einhaltung der für Ottobock verbindlichen rechtlichen Regelungen und Vorgaben zum Datenschutz sowie deren Konkretisierung im Rahmen von Ottobock-internen Regelwerken verstanden. Die unternehmerischen Handlungen stehen dabei auch in Übereinstimmung mit den internen Regeln, die von allgemeinen gesellschaftlichen Wertvorstellungen sowie von Moral und Ethik geprägt sind. Die Gewährleistung von „Datenschutz-Compliance“ ist die Aufgabe eines jeden, vom Aufsichtsrat, Verwaltungsrat zu den geschäftsführenden Direktoren, den Führungskräften und eines jeden einzelnen Mitarbeiters von Ottobock.

2. Grundelemente des Data Privacy Management Systems von Ottobock

Zielsetzung des DPMS von Ottobock ist es, mit einem systematischen Rahmen regelkonformes Verhalten zu erreichen und Datenschutz-Risiken zu minimieren. Der Umfang des DPMS bemisst sich durch die Summe aller datenschutzrelevanten Maßnahmen. Die Maßnahmen werden risikoorientiert abgeleitet und sind sowohl zentral beim Fachbereich Data Privacy als auch dezentral in sämtlichen Fachbereichen von Ottobock angesiedelt.

Das DPMS bildet zudem einen einheitlichen aufbau- und ablauforganisatorischen Rahmen für alle datenschutz-relevanten Themengebiete, denen wesentliche Datenschutz-Risiken innewohnen: Es schafft somit eine Struktur, um Maßnahmen zur Einhaltung der rechtlichen Regelungen und Vorgaben in den jeweiligen Datenschutz Fokusthemen prozessual und methodisch effektiv und effizient umsetzen zu können. Zudem werden Standards geschaffen, um Mindestanforderungen für datenschutz-relevante Prozesse, Verfahren etc. zu etablieren. Hierzu zählt z.B. die Schaffung von Standards bei der Identifikation von Compliance-Risiken durch die Fachbereiche oder für die Erstellung von Compliance-Schulungen.

Das DPMS von Ottobock orientiert sich in seinem Aufbau grundsätzlich an dem Prüfungsstandard „IDW PS 980“ sowie insbesondere in der inhaltlichen Ausgestaltung am Prüfungsstandard „IDW PS 986.1“, welche vom Institut der Wirtschaftsprüfer veröffentlicht wurde. In Anlehnung an diesen Standard unterteilt sich das DPMS von Ottobock in die folgenden sieben Elemente. Diese Elemente bilden die Grundlage für die unternehmensspezifische Ausgestaltung und Operationalisierung des DPMS:

- Datenschutz-Kultur
- Datenschutz-Ziele
- Datenschutz-Organisation
- Datenschutz-Risiken
- Datenschutz-Programm
- Datenschutz-Kommunikation

[1] Hiervon zu unterschieden sind die in anderen Compliance Management Systemen (z.B. Tax Compliance Management System und (Legal-) Compliance Management System) gemanagten Compliance-Risiken.

- Datenschutz-Überwachung und Verbesserung

B. DATENSCHUTZ-KULTUR

Die Basis eines funktionierenden DPMS ist die gelebte Datenschutz-Kultur im Unternehmen. Sie wird vor allem geprägt durch die Grundeinstellungen und Verhaltensweisen der Geschäftsführung sowie der Aufsichtsorgane („Tone from the Top"). Die Datenschutz-Kultur beeinflusst die Bedeutung, welche die Mitarbeiter des Unternehmens der Beachtung von datenschutzbezogenen Regeln beimessen und damit die Bereitschaft zu datenschutzkonformem Verhalten. Für Ottobock sind in diesem Zusammenhang die Unternehmenswerte und der davon abgeleitete Code of Conduct von besonderer Bedeutung.

1. Code of Conduct

Mit dem Code of Conduct bekennen sich die Anteilseigner, insbesondere die Familie Näder, der Aufsichtsrat, der Verwaltungsrat und die geschäftsführenden Direktoren sowie der Betriebsrat zu den Grundwerten der Unternehmenskultur von Ottobock. Der Code of Conduct dient innerhalb der Ottobock-Gruppe als verbindliche Grundlage für das Verhalten aller Mitarbeiter (mit und ohne Führungsverantwortung) sowie der Geschäftsführung im Geschäftsalltag.

Der Code of Conduct wurde von der Geschäftsführung erarbeitet und vom Verwaltungsrat nach Zustimmung des Aufsichtsrats verabschiedet. Die Geschäftsführungen aller[2] Tochterunternehmen der Ottobock SE & Co. KgaA haben den Code of Conduct, auf Wunsch des CEO, für die in ihrem Verantwortungsbereich stehenden Gesellschaften ebenfalls verabschiedet und implementiert. Der Code of Conduct der Ottobock SE & Co. KgaA ist in deutscher und englischer Sprache im Intranet sowie auf der Internetseite des Unternehmens abrufbar.

Der Code of Conduct bekennt sich in Ziffer 8 zur Einhaltung des Datenschutzes:

> **„Sensible Informationen sind diskret zu behandeln**
> Der Schutz vertraulicher, geheimer und personenbezogener Daten gehört zu den Grundsätzen in allen Beziehungen zu Kollegen (auch ehemaligen) sowie deren Angehörigen, Bewerbern, Kunden, Lieferanten und sonstigen Personenkreisen.
>
> Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, soweit dies für klar definierte und rechtmäßige Zwecke erforderlich ist. Unser Unternehmen stellt sicher, dass die Verwendung der Daten für die Betroffenen transparent ist und ihre Rechte auf Auskunft und Berichtigung gewahrt werden.
>
> Jeder Mitarbeiter ist verpflichtet, die datenschutzrechtlichen Bestimmungen sowie die gesetzlichen und betrieblichen Regelungen zur Informationssicher-

[2] Hiermit sind alle Tochterunternehmen der Ottobock SE & Co. KGaA gemeint, an denen diese mit mehr als 50% beteiligt ist (Mehrheitsbeteiligung).

heit einzuhalten und die unserem Unternehmen anvertrauten Daten vor missbräuchlicher Verwendung zu schützen. Unser Unternehmen verpflichtet sich, einen angemessenen Standard bei der Absicherung der Informationsverarbeitung zu gewährleisten. Alle Komponenten der Informationsverarbeitung müssen so sicher sein, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit der schützenswerten Informationen gegeben und eine unbefugte interne oder externe Nutzung verhindert wird.

Geschäfts- oder Betriebsgeheimnisse sind streng vertraulich. Dieser Grundsatz ist auch für den Schutz der Informationen unserer Geschäftspartner zu beachten. Über Arbeits- und Geschäftsvorgänge im Unternehmen, die für unser Unternehmen oder Geschäftspartner sensibel sind, ist Stillschweigen zu bewahren. Die direkte oder indirekte Nutzung nicht öffentlicher Geschäftsinformationen zum persönlichen Vorteil, zum Vorteil Dritter oder zum Nachteil unseres Unternehmens ist unter-sagt.

Geistiges Eigentum ist für den Erfolg und die wirtschaftliche Entwicklung von Otto-bock unerlässlich. So ist unser geistiges Eigentum zu schützen, einschließlich aller Patente, Marken und Urheberrechte, Geschäftsgeheimnisse, technische und wissenschaftliche Kenntnisse und das im Laufe der Jahre entwickelte Know-how unseres Unternehmens. Umgekehrt respektiert Ottobock auch das geistige Eigentum anderer.

Die Verpflichtung zur Einhaltung aller zuvor genannten Punkte gilt über die Dauer des aktiven Beschäftigungsverhältnisses hinaus.“

2. „Tone from the Top“

Das Vorbildverhalten der Geschäftsführung in Bezug auf das Einhalten bzw. der Berücksichtigung der Unternehmenswerte sowie der geltenden internen und externen Regelungen zum Datenschutz ist für die Bildung einer starken Datenschutz-Kultur bei Ottobock wichtig. Das Vorleben der Einhaltung der Regelungen zum Datenschutz ist die Basis, um alle Mitarbeiter zu motivieren, die Datenschutz-Kultur mitzuprägen und regelkonform zu handeln.

Der „Tone from the Top“ für das Thema Datenschutz konkretisiert sich bei Ottobock durch Beiträge der Geschäftsführung zur Einhaltung der Unternehmenswerte und geltenden rechtlichen Regelungen und Vorgaben zum Datenschutz sowie durch weitere Maßnahmen. Hierzu zählen zum Beispiel die Unterstützung und Bereitstellung von Ressourcen für die Implementierung von notwendigen Datenschutz-Maßnahmen durch die Fachbereiche, die Mitgliedschaft eines Mitglieds der Geschäftsleitung im Data Privacy Management Committee (DPMC), Kommunikationsmaßnahmen zu bestimmten ggf. tagesaktuellen Datenschutz-Themen oder auch das Anhalten der Verantwortlichen der weiteren Ottobock-Gesellschaften zur Umsetzung von Datenschutzvorgaben-Vorgaben.

Die Gesamtheit der Maßnahmen der Geschäftsführung und der damit verbundene Beitrag zur Stärkung der Datenschutz-Kultur wird als „Tone from the Top“ bezeichnet.

3. Beratung und verpflichtende Einbindung des Fachbereichs Data Privacy

Die Beratung der Geschäftsführung und der Fachbereiche im Hinblick auf datenschutz-relevante Aspekte ist eine Kernaufgabe des Fachbereichs Data Privacy.[3] Zur angemessenen Erfüllung der Beratungsaufgabe ist der Fachbereich Data Privacy bei datenschutz-relevanten Sachverhalten mit dem Ziel einzubinden, diesem ein präventives Agieren zu ermöglichen und darauf hinzuwirken, dass zu treffende Entscheidungen, Kommunikationsmaßnahmen sowie Dokumente im Einklang mit den geltenden rechtlichen Regelungen und Vorgaben ausgestaltet sind.

Zu den datenschutz-relevanten Sachverhalten, bei denen der Fachbereich Data Privacy beratend einzubinden ist, gehören insbesondere

- die Bearbeitung von Beschwerden durch die zuständigen Fachbereiche in datenschutz-relevanten Themengebieten,
- die Kommunikation durch den Fachbereich Unternehmenskommunikation mit Vertretern der Presse zu Datenschutz Fokusthemen und
- die Kommunikation mit Behörden zu datenschutz-relevanten Sachverhalten durch den Fachbereich Data Privacy (als ein Teilbereich des Fachbereichs Cyber Security).

Darüber hinaus kann der Fachbereich Data Privacy im Rahmen der Entwicklung von Grundsätzen und Prozessen sowie der Erstellung und Weiterentwicklung interner Organisations- und Arbeitsanweisungen mit Bezug zu Datenschutz Fokusthemen durch die Fachbereiche beratend hinzugezogen werden.

Die Definition von Datenschutz Fokusthemen ist im Gliederungspunkt 2. Dargestellt.

Um Compliance-Risiken vollumfänglich und frühzeitig begegnen zu können, soll der Fachbereich Data Privacy künftig auch bei den folgenden Sachverhalten, sofern eine Compliance-Relevanz gegeben ist, eingebunden werden:

- Begleitung in neue Märkte,
- strategische Unternehmensentscheidungen,
- betriebliche Veränderungen und
- geplante Eingliederungen und Auslagerungen, welche im Zusammenhang mit den Datenschutz Fokusthemen (vgl. hierzu Gliederungspunkt 2.) stehen.

4. Anreizsystem & Verbesserungsprozess

Ein Anreizsystem dient insbesondere dazu, die Entwicklung einer positiven Compliance-Kultur zu fördern. Dabei können unterschiedlichste Maßnahmen dazu dienen, regelkonformes Verhalten nachhaltig zu fördern. Die Hoheit sowohl über den konzeptionellen und methodischen Rahmen als auch die Umsetzung damit verbundener Maßnahmen liegt bei Global HR.

Zielsetzung des Verbesserungsprozess ist die Schaffung von Leitlinien und einheitlichen Prozessen für den Umgang mit unbewusstem Fehlverhalten und bewussten bzw. vorsätzlichen Regelverstößen.

[3] Die gesetzlich vorgesehene Beratungsaufgabe des betrieblichen Datenschutzbeauftragten wird durch diese Aufgabenzuweisung nicht eingeschränkt.

Für den Erfolg von Ottobock ist unter anderem auch das Lernen aus Fehlern, insbesondere aus unbewusstem Fehlverhalten, unerlässlich, wodurch die „Fehlerkultur“ integraler Bestandteil der Compliance-Kultur ist. Für unbewusste Compliance-Verstöße gilt der Leitsatz Otto Bocks:

> *„Ermuntere den anderen, Fehler zu beseitigen, selbst etwas zu unternehmen und sich zu entscheiden.“*
> [Otto Bock, 1944]

Für vorsätzliches Fehlverhalten und bewusste Compliance-Verstöße hingegen gilt das „zero tolerance-Prinzip“. Das konsequente Handeln und Sanktionieren in diesen Fällen ist notwendig, um die Compliance-Kultur bei Ottobock zu stärken und aufrechtzuerhalten.

Der Fachbereich Global HR hat zum Umgang mit Fehlverhalten und bewussten Datenschutz-Verstößen Vorgaben definiert. Die Vorgaben sollen einen einheitlichen Rahmen für den Umgang mit und die Festlegung von arbeitsrechtlichen Konsequenzen[4] bilden und einer objektiven, durch Dritte nachvollziehbaren, Beurteilung dienen. Auch wenn jeder Sachverhalt einer Einzelfallbetrachtung bedarf, ist ein einheitlicher Rahmen unerlässlich, um einen fairen und gerechten Umgang bei vergleichbaren Compliance-Vorfällen zu erreichen.

C. DATENSCHUTZ-ZIELE

Im Rahmen der Festlegung von Compliance-Zielen unterscheidet Ottobock die nachfolgenden zwei Aspekte:

1. Definition konkreter DPMS-Ziele

Zum einen werden die Ziele, die mit dem DPMS verfolgt werden, definiert und beschrieben. Diese Ziele sind mit den Unternehmenszielen von Ottobock abgestimmt und fördern diese. Die übergeordneten Ziele des DPMS bei Ottobock sind:

1. Aktives und effizientes Steuern von Datenschutz-Risiken durch die Schaffung
   methodischer Ansätze für operative Verantwortlichkeiten.
2. Schaffung eines Rahmens zur Förderung von datenschutzkonformen Verhalten
3. Förderung und Pflege der Datenschutz-Kultur und Beitrag zu einer guten Unternehmens-Governance
4. Ausgestaltung eines organisatorischen Rahmenwerks für datenschutzrelevante Themengebiete
5. Beitrag zum Unternehmenserfolg durch die Ermöglichung einer nachhaltigen Nutzung von Daten zur Verbesserung unserer Produkte und Services der Patientenversorgung

Die Ziele des DPMS werden in Abhängigkeit der fortwährenden Weiterentwicklung des DPMS in regelmäßigen Abständen durch den Fachbereich Data Privacy und den

betrieblichen Datenschutzbeauftragten, in Abstimmung mit der Geschäftsführung, überprüft und entsprechend des Reifegrads des DPMS von Ottobock angepasst.

2. Festlegung Datenschutz-Fokusthemen

Zum anderen werden Datenschutz Fokusthemen bei Ottobock festgelegt. Hierbei handelt es sich um Themengebiete, die wesentliche Datenschutz-Risiken beinhalten können und denen somit eine hohe Bedeutung für ein angemessenes und wirksames Management der Compliance-Risiken zukommt. Die Datenschutz-Fokusthemen finden Berücksichtigung im Rahmen des Compliance-Programms und werden in die Datenschutze-Risikoanalyse einbezogen. Das DPMS gibt für diese Datenschutz Fokusthemen den methodischen und organisatorischen Rahmen vor, welches für jedes Datenschutz-Fokus-Thema Anwendung findet. Auf diese Weise können Schnittstellen genutzt und Synergien gehoben werden.

Für Ottobock werden die nachfolgend in der Tabelle aufgeführten Datenschutz Fokusthemen als wesentlich angesehen. Der für ein Datenschutz-Fokus-Thema jeweils verantwortliche Fachbereich ist ebenfalls in der Tabelle aufgeführt. Um den Compliance-Risiken, die in diesen Themengebieten entstehen, entsprechend Rechnung zu tragen, ist aus den verantwortlichen Fachbereichen für jedes Themengebiet ein **Datenschutz-Koordinator** benannt (siehe Gliederungspunkt 8.).

Datenschutz-Fokus-Thema	**Verantwortlicher Fachbereich**
Datenschutz im Beschäftigungsverhältnis	Global HR-Management (Leitung Global HR-Management)
Datenschutz in der Informationstechnik	Global IT (Leitung Global IT)
Datenschutz Patient Care	Patient (Leitung Patient Care)
Datenschutz in Forschung und Entwicklung	Global Research and Develeopment (Lei-tung Research and Develeopment)
Datenschutz in Clinical Research	Clinical Research (Leitung Clinical Research)
Datenschutz in der Marktforschung	Global O&P Solutions (Leitung Global O&P Solutions)
Datenschutz Marketing Technologies	Marketing-Technologies (Leitung Marketing Technologies)
Datenschutz Digital Health Solution	Digital Health Solution (Leitung Health Solution als Teilbereich von Marketing-Technologies)

Die Datenschutz-Fokusthemen werden in regelmäßigen Abständen überprüft und ggf. aktualisiert. Ein Grund hierfür ist, dass die datenschutz-relevanten Themengebiete auch die Ausgangsbasis für die Betrachtung der Compliance-Risiken darstellen. Somit ist die Aktualität der datenschutz-relevanten Themengebiete essenziell, um auf Basis dieser die Compliance-Risikosituation von Ottobock adäquat ermitteln zu können.

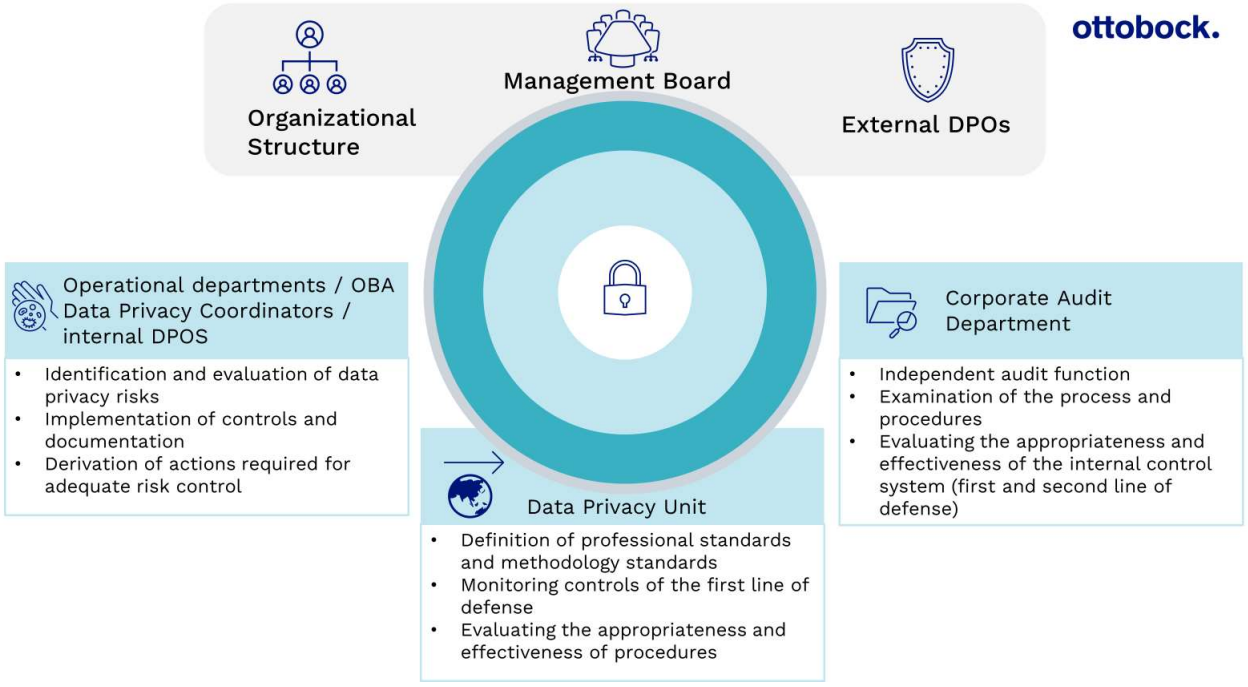
D. DATENSCHUTZ-ORGANISATION

Datenschutz betrifft das gesamte Unternehmen. Um eine wirksame Compliance-Organisation einzurichten und aufrechtzuerhalten, ist eine angemessene Governance-Struktur im Unternehmen notwendige Voraussetzung. Ottobock orientiert sich hierbei am Modell der drei (Verteidigungs-)Linien.

Die Gesamtverantwortung für Datenschutz-Management liegt bei allen geschäftsführenden Direktoren in ihrer Gesamtheit. Organisatorisch ist der Fachbereich Data Privacy dem Ressort des CXO und dort der Global IT zugeordnet und mit einer direkten Berichtslinie an den CXO ausgestattet. Unterstützt werden der CXO und der Fachbereich Data Privacy durch die Datenschutz-Koordinatoren, welche für die oben aufgeführten Datenschutz Fokusthemen benannt sind.

Daneben hat die Ottobock SE & Co. KGaA einen externen betrieblichen Datenschutzbeauftragten benannt. Der betriebliche Datenschutzbeauftragte berichtet direkt an den CXO. Der Fachbereich Data Privacy kooperiert mit dem betrieblichen Datenschutzbeauftragten. Coorperate Audit übt in diesem Zusammenarbeitsmodell eine unabhängige Kontrollfunktion aus-.

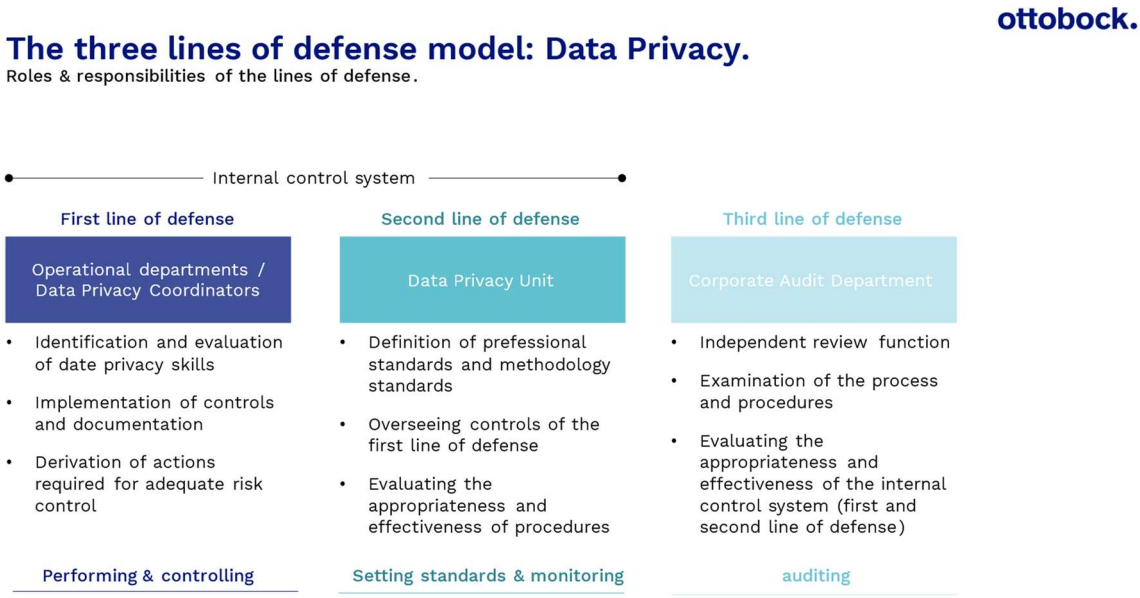
Vereinfachte Darstellung der Datenschutz-Organisation von Ottobock:



1. Modell der drei (Verteidigungs-)Linien als zentrales Organisationsprinzip

Das Modell der drei (Verteidigungs-)Linien schafft den strukturellen Rahmen für die effektive Steuerung von (Datenschutz-) Risiken in einem Unternehmen. Darüber hinaus ist es ein wichtiger Eckpfeiler zur Stärkung des Datenschutz-Bewusstseins und der Datenschutz-Kultur. Im Folgenden wird das Modell aus der Datenschutz-Management-Perspektive erläutert.

Die Einführung des Organisationsprinzips der drei (Verteidigungs-)Linien bei Ottobock soll der frühzeitigen Erkennung und der angemessenen und wirksamen fachbereichsübergreifenden Steuerung von Datenschutz-Risiken dienen, um zum Beispiel Datenschutz-Vorfälle und die damit ggf. verbundenen Schäden zu verhindern bzw. gering zu halten. In diesem Zusammenhang verfolgen die erste und zweite (Verteidigungs-)Linie einen systematischen, methodisch basierten Ansatz, um implementierte Verfahren und Maßnahmen zur Abwehr von Datenschutz-Risiken zu bewerten und potenziellen Handlungsbedarf identifizieren zu können.



Hinweis: Es können auch weitere/andere Fachbereiche als zweite (Verteidigungs-)Linie fungieren (z.B. Risikomanagement oder Legal Compliance). Auf eine Darstellung dieser wurde in der Abbildung verzichtet, da diese das Modell nur aus Compliance-Perspektive darstellt

Dem Modell folgend werden die bei Ottobock bestehenden Organisationseinheiten jeweils einer der drei (Verteidigungs-)Linien zugeordnet. Jede Linie nimmt dabei unterschiedliche Aufgaben wahr: Die Führungskraft und die Mitarbeiter jedes operativen Fachbereichs sind dafür verantwortlich, die in ihrem Fachbereich relevanten Compliance-Risiken zu identifizieren und diese angemessen und wirksam zu steuern (*erste (Verteidigungs-)Linie*). Der Fachbereich Data Privacy als *zweite (Verteidigungs-)Linie* setzt Mindeststandards für ein angemessenes und wirksames Compliance-Risikomanagement. Darüber hinaus wirkt der Fachbereich Data Privacy auf die Angemessenheit und Wirksamkeit des Kontrollgefüges hin. Die erste und zweite (Verteidigungs-)Linie bilden somit das interne Kontrollsystem (IKS). Corporate Audit bildet nachgelagert, als unabhängige Prüfungsinstanz, die *dritte (Verteidigungs-)Linie*. Diese überprüft ganzheitlich die Ausgestaltung des IKS und somit die erste und zweite (Verteidigungs-)Linie.

Für den betrieblichen Datenschutzbeauftragen gilt das für den Fachbereich Data Privacy ausgeführte entsprechend.

2. Rolle & Verantwortlichkeit der ersten (Verteidigungs-) Linie

Jeder Fachbereich der ersten (Verteidigungs-)Linie trägt die Verantwortung für die Datenschutz-Risiken im eigenen Fachbereich *(Risk Owner)* und übernimmt u.a. folgende Aufgaben:

- Identifikation von Datenschutz-Risiken im Fachbereich auf Basis der vom Fachbereich Data Privacy festgelegten Vorgaben zu Datenschutz-Standards.
- Steuerung der Datenschutz-Risiken im eigenen Fachbereich, durch:
    - Fachbereichsspezifische Konkretisierung von der Datenschutz-Standards (sofern notwendig)
- Sicherstellung der Einhaltung von relevanten internen/externen Regelungen, durch Implementierung von Prozessen, Maßnahmen, Arbeitsanweisungen etc. z.B. Pflege der Verfahrensverzeichnisse. Ggf. Identifizierung von Datenschutz-Risiken im Rahmen der Durchführung einer Datenschutz-Risikoanalyse und ggf. Durchführung von Datenschutzfolgeabschätzungen.
    - Identifizierung Datenschutz-relevanter Prozesse (vgl. hierzu datenschutz-relevante Themengebiete in Gliederungspunkt 2.)
    - Einrichtung prozessorientierter Kontrollmechanismen und regelmäßige Durchführung von (risikobasierten) Kontrollen, um feststellen zu können, ob die implementierten Maßnahmen umgesetzt werden und damit den verfolgten Zweck erfüllen. Die Form der Kontrolldokumentation obliegt grundsätzlich den operativen Fachbereichen; folgende Informationen sind jedoch mindestens zu dokumentieren:
        - Name der Kontrolle
        - Beschreibung der Kontrolle
        - Zugrundeliegende/r Prozess/Maßnahme
        - Umfang
        - Turnus
        - Ergebnis
        - Abgeleiteter Handlungsbedarf
        - Datum der Kontrolle und Name der kontrollierenden Person
    - Ableitung von Handlungserfordernissen, sofern im Rahmen von Kontrollhandlungen etwaiges Verbesserungspotenzial identifiziert wurde.
    - Dokumentation der identifizierten Datenschutz-Risiken, geplanten und durchgeführten Kontrollen sowie risikoreduzierenden Maßnahmen
    - Berichterstattung zu Datenschutz-Risiken sowie risikoreduzierenden Maßnahmen an den Fachbereich Data Privacy
    - Ad-hoc Berichterstattung an den Fachbereich Data Privacy bei Erkennen von wesentlichen neuen, geänderten Datenschutz-Risiken sowie Verdachtsfällen oder identifizierten Datenschutz-Verstößen

3. Rolle & Verantwortung der zweiten (Verteidigungs-)Linie

3.1 Fachbereich Data Privacy

Der Fachbereich Data Privacy nimmt im Rahmen des Modells der drei (Verteidigungs-)Linien im Wesentlichen folgende Aufgaben auf der zweiten (Verteidigungs-)Linie wahr:

- Vorgabe von Datenschutz-Standards sowie ggf. Anstoßen der Implementierung durch die verantwortlichen Fachbereiche, um die erste (Verteidigungs-)Linie bei der Durchführung ihrer Aufgaben fachlich zu unterstützen
- Begleitung und ggf. Anstoß der Datenschutz-Risikoanalyse und, gemeinsam mit den Datenschutz-Koordinatoren,
- Begleitung sowie Beratung der Fachbereiche im Rahmen der Durchführung und anschließende Validierung der Ergebnisse
- Beratung des betrieblichen Datenschutzbeauftragten bei der Planung und Durchführung von risikoorientierten Überwachungshandlungen, um beurteilen zu können, ob die erste (Verteidigungs-)Linie entsprechende Verfahren, Maßnahmen und Kontrollen implementiert hat, um in angemessener und wirksamer Weise den jeweils relevanten Datenschutz-Risiken entgegenzuwirken
- Beratung der Fachbereiche bei datenschutz-relevanten Sachverhalten
- Bereitstellung von Informationen an Corporate Audit, damit die Interne Revision der Aufgabe als dritte (Verteidigungs-)Linie nachkommen kann
- Jährlicher Austausch mit Corporate Audit hinsichtlich der geplanten Aktivitäten im Rahmen des Überwachungsplans und des Prüfungsplans, um insbesondere zeitliche Überschneidungen in gleichen Themengebieten zu vermeiden
- Regelmäßige Berichterstattung an die Geschäftsführung
- Ad-hoc Berichterstattung an die Geschäftsführung bei Erkennen von wesentlichen neuen, geänderten Datenschutz-Risiken und/oder Regelungen sowie Verdachtsfällen oder identifizierten Datenschutz-Verstößen
- Zusammenarbeit mit Aufsichtsbehörden in Abstimmung mit dem Betrieblichen Datenschutzbeauftragten

.

3.2 Externer Betrieblicher Datenschutzbeauftragter

Der externe Betriebliche Datenschutzbeauftragte übernimmt die gesetzlichen Aufgaben eines Datenschutzbeauftragten gemäß Art. 39 DSGVO:

- Unterrichtung und Beratung von Ottobock und dessen Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Europäischen Union bzw. der Mitgliedstaaten
- Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Europäischen Union bzw. der Mitgliedstaaten, sowie der Strategien von Ottobock für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und regelmäßige Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- auf Anfrage Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO
- Tätigkeit als Kontaktstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und gegebenenfalls Beratung zu allen sonstigen Fragen.

Der betriebliche Datenschutzbeauftragte handelt bei der Ausübung seiner Tätigkeiten nach Art. 38 und 39 DSGVO weisungsfrei.

4. Rolle & Verantwortung der dritten (Verteidigungs-)Linie – Corporate Audit

Aufgabe der dritten (Verteidigungs-)Linie ist es, insbesondere im Rahmen von unabhängigen Audits die Einhaltung von rechtlichen Regelungen und Vorgaben sowie diese konkretisierenden, internen Regelwerke der ersten und zweiten (Verteidigungs-)Linie zu überprüfen und damit die Angemessenheit und Wirksamkeit des Datenschutz- und des Risikomanagements im Allgemeinen sowie des internen Kontrollsystems im Besonderen zu beurteilen.

In der Regel erfolgen die Prüfungen des Bereichs Corporate Audit als Interne Revision nachgelagert und prozessunabhängig.

Eine Übersicht der Schnittstellen zwischen dem Fachbereich Data Privacy und Corporate Audit befindet sich im Anhang Schnittstellenvereinbarung mit der dritten , Seite L.5 ff.

5. Ressortzuständigkeit Chief Experience Officer

Der Fachbereich Data Privacy liegt im Verantwortungsbereich des CXO. Insoweit übernimmt er eine Führungsverantwortung innerhalb der Datenschutz-Organisation. Wichtige Grundsatzentscheidungen bezüglich des Datenschutzmanagements sind durch ihn vorzunehmen bzw., sofern die Zustimmung weiterer Geschäftsführungsmitglieder notwendig ist, durch ihn mitzutragen. Zudem ist er verantwortlich dafür, die grundlegenden Standards (z.B. diese Policy) freizugeben bzw. sie unternehmensweit zu veröffentlichen. Ein regelmäßiger Informationsfluss ist im Rahmen von Jour Fixe-Termine gegeben und zudem dadurch gesichert, dass der CXO des Data Privacy Management Committees (DPMC) ist. Darüber hinaus erhält er regelmäßige Berichterstattungen durch den Fachbereich Data Privacy (vgl. hierzu Gliederungspunkt F.3) und den Betrieblichen Datenschutzbeauftragten.

6. Fachbereich Data Privacy

6.1 Organisation

Der Fachbereich Data Privacy ist ein Teilbereich des Fachbereichs Cyber Security, der Datenschutz-Aufgaben wahrnimmt. Er besteht aus dem Head of Data Privacy und den mit Datenschutz-Aufgaben betrauten Mitarbeitern des Fachbereichs.

6.2 Kernaufgaben

Die Kernaufgaben des Fachbereichs Data Privacy im Zusammenhang mit dem DPMS umfassen insbesondere die Folgenden:

- Beratung der Fachbereiche bei der Einrichtung von datenschutz-relevanten Prozessen Richtlinien und Anweisungen,
- Erarbeitung von Datenschutz-Zielen zur Vorlage und Entscheidung durch die Geschäftsführung
- Beratung der Geschäftsführung und der Fachbereiche zu datenschutz-relevanten Fragestellungen (vgl. hierzu Gliederungspunkt 3.)
- Entwicklung von Maßnahmen zur fortwährenden Stärkung der Datenschutz-Kultur und Steigerung des Datenschutz-Bewusstseins

- Förderung des Austauschs zu rechtlichen Änderungen bzw. Neuerungen in allen Datenschutz Fokusthemen mit den Datenschutz-Koordinatoren en und Durchführung des Rechtsmonitorings bei selbst verantworteten Datenschutz-relevanten Themengebieten
- Beratung des Betrieblichen Datenschutzbeauftragten bei der Durchführung von risikoorientierten Überwachungshandlungen im Rahmen der Funktion als zweite (Verteidigungs-)Linie (vgl. hierzu Gliederungspunkt 3)
- Unterstützung des betrieblichen Datenschutzbeauftragten bei der Aufnahme und Bewertung von anonymen oder vertraulichen Hinweisen und bei Bedarf Veranlassung weiterer Untersuchungs- oder Abhilfemaßnahmen.
- Unterstützung des betrieblichen Datenschutzbeauftragten bei Vorliegen eines Anfangsverdachts auf Datenschutz-Verstöße erfolgt eine Empfehlung an die Geschäftsführung zur Durchführung von internen Ermittlungen durch die dritte (Verteidigungs-)Linie oder Dritte (z.B. Wirtschaftsprüfungsgesellschaften)
- Unterstützung des betrieblichen Datenschutzbeauftragten bei der regelmäßigen Prüfung auf Anpassungsbedarf des Schulungskonzepts (methodischer Rahmen) für Datenschutz-Schulungen, in Zusammenarbeit mit dem Fachbereich HR
- Hinwirken auf die Durchführung von Schulungen in den Datenschutz Fokusthemen und Durchführung eigener Schulungen in den selbst verantworteten datenschutz-relevanten Themengebieten
- Initiierung gezielter Kommunikationsmaßnahmen zu datenschutz-relevanten Sachverhalten
- Regelmäßige Information an den CXO durch Austausch im DPC und im Rahmen von Jour Fixe-Terminen
- Regelmäßige Berichterstattung über datenschutz-relevante Risiken, Aktivitäten und Sachverhalte an die Geschäftsführung

Zur ordnungsgemäßen Erfüllung der Kernaufgaben nehmen die Mitarbeiter des Fachbereichs Datenschutz-Management zudem regelmäßig (in der Regel jährlich) an Fortbildungen teil.

6.3 Rechte und Kompetenzen

Um die mit dem DPMS verbundenen Aufgaben wahrnehmen zu können, wurden dem Fachbereich Data Privacy seitens der Geschäftsführung verschiedene Rechte und Kompetenzen übertragen. Die im folgenden aufgeführten Rechte und Kompetenzen gelten innerhalb der Ottobock SE & Co. KGaA.

Eskalationsrecht

Der Fachbereich Data Privacy hat das Recht, datenschutz-relevante Sachverhalte gegenüber der Geschäftsführung und ggf. dem Aufsichtsrat zur Entscheidung vorzulegen. Dies kann je nach Relevanz und Dringlichkeit sowohl im Rahmen einer regelmäßigen Berichterstattung bzw. anderer wiederkehrender Termine als auch ad-hoc erfolgen.

Informationsrecht

Der Fachbereich Data Privacy hat ein umfassendes Informationsrecht über alle datenschutz-relevanten Sachverhalte (etwa in Form eines Berichts), die von den Fachbereichen auf Nachfrage zur Verfügung zu stellen sind. Für den Fall, dass an-

geforderte, notwendige Informationen seitens des Fachbereichs nicht zur Verfügung gestellt werden, verfügt der Fachbereich Data Privacy über ein Eskalationsrecht (siehe oben). Die Verwendung der Daten und Informationen sind dem Fachbereich Data Privacy ausschließlich zur Erfüllung seiner Datenschutz-Aufgaben gestattet und werden streng vertraulich behandelt.

Überwachungsrecht (Unterstützung des Betrieblichen Datenschutzbeauftragten)

Der Fachbereich Data Privacy ist gemäß dem Organisationsprinzip der drei (Verteidigungs-)Linien verpflichtet, den Betrieblichen Datenschutzbeauftragten bei der Vornahme risikobasierter Überwachungshandlungen im Rahmen der Funktion als zweite (Verteidigungs-)Linie (vgl. hierzu Gliederungspunkt 3) zu unterstützen. Zur Erfüllung dieser Aufgabe ist der Fachbereich Data Privacy mit den oben genannten Informationsrechten ausgestattet. Im Rahmen dieser Tätigkeit unterstützt der Fachbereich Data Privacy den Betrieblichen Datenschutzbeauftragten fachlich. Auf Basis der Ergebnisse werden bei Bedarf von den Fachbereichen abgeleitet, um die Datenschutz-Risiken weiter zu reduzieren. Darüber hinaus sind die Ergebnisse der Überwachungshandlungen Bestandteil der regelmäßigen Berichterstattung des Fachbereichs Datenschutz-Management und des Betrieblichen Datenschutzbeauftragten an die Geschäftsführung.

Votumsrecht

Der Fachbereich Data Privacy kann empfehlen, einzelne geschäftliche oder vertriebliche Aktivitäten, Geschäftsbeziehungen oder ähnliches abzulehnen, wenn einschlägige rechtliche Regelungen und Vorgaben oder diese konkretisierenden Ottobock-interne Vorgaben nicht erfüllt sind. Sollte der Fachbereich der Empfehlung nicht folgen, steht dem Fachbereich Data Privacy ein Eskalationsrecht zu (siehe oben).

6.4 Organisationsvereinbarungen zwischen 1. und 2. Verteidigungslinie

Die 1. und 2. Verteidigungslinie treffen Organisationsvereinbarungen auf Basis der in diesem Gliederungspunkt beschriebenen Datenschutzorganisation. Dazu legt der Fachbereich Data Privacy Datenschutz-Fokusthemen (Gliederungspunkt 8.) fest, um die innerorganisatorische Abgrenzung und Verantwortlichkeit zu gewährleisten.

7. Betrieblicher Datenschutzbeauftragter

Dem betrieblichen Datenschutzbeauftragten kommen die gesetzlich zugewiesenen Aufgaben und Pflichten zu (vgl. hierzu auch Ziff. 3.2).

Diese Aufgaben beinhalten die folgenden Rechte:

- **Eskalationsrecht**
- **Informationsrecht**
- **Überwachungsrecht**
- **Votumsrecht**

Der betriebliche Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt (Art. 39 Abs. 2 DSGVO).

Der Fachbereich Datenschutz Management unterstützt den betrieblichen Datenschutzbeauftragten bei der Ausübung seiner Tätigkeit.

Der betriebliche Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Art. 38 Abs. 5 DSGVO).

8. Datenschutz-Koordinatoren

Als Datenschutz-Koordinator wird in der Regel der Leiter des Fachbereichs benannt.

Die Ernennung erfolgt in Form einer gegenseitigen Vereinbarung und wird Bestandteil der Personalakte. Damit wird der Datenschutz-Koordinator Bestandteil der Datenschutz-Organisation von Ottobock. Die Rolle als Datenschutz-Koordinator kann von Bereichsleitern hierarchisch weiter delegiert werden.

Für den Fachbereich Data Privacy fungieren die Datenschutz-Koordinatoren als operativ Verantwortliche zu datenschutz-relevanten Sachverhalten. Tätigkeitsschwerpunkt des Datenschutz-Koordinators ist es, die Umsetzung der datenschutzrechtlichen Vorgaben anzustoßen, zu koordinieren, auf die angemessene und wirksame Ausgestaltung sowie die kontinuierliche risikoorientierte Weiterentwicklung des DPMS im jeweilig zugewiesenen datenschutz-relevanten Themengebiet hinzuwirken. Der Fachbereich Data Privacy handelt im Auftrag der Geschäftsführung und gibt in diesem Zusammenhang rechtliche, methodische und organisatorische Vorgaben. Die Datenschutz-Koordinatoren berücksichtigen diese Vorgaben bei der fachlichen Umsetzung.

Zu den Aufgaben des Datenschutz-Koordinators im Zusammenhang mit dem zugewiesenen datenschutz-relevanten Themengebiet gehören insbesondere:

- die Beratung der Mitarbeiter der Fachbereiche hinsichtlich datenschutz-relevanter Fragestellungen im Zusammenhang mit dem datenschutz-relevanten Themengebiet (fungieren als erster Ansprechpartner)
- das Vorantreiben der Umsetzung (neuer) rechtlicher Anforderungen und Behebung festgestellter Defizite
- die Erstellung von Standards, Anweisungen, Prozessen etc. zur Einhaltung der Vorgaben
- die Mitwirkung bei der Vorbereitung, Durchführung und Validierung der Datenschutz-Risikoanalyse
- die Unterstützung im Rahmen der Ableitung und die Verantwortung für die Durchführung von Kontrollhandlungen
- die Unterstützung bzw. Vorbereitung im Rahmen der Durchführung von risikoorientierten Überwachungshandlungen durch den Fachbereich Data Privacy
- die Durchführung von Schulungs- und Kommunikationsmaßnahmen

- die Unterstützung des Fachbereichs Data Privacy im Rahmen der Bearbeitung von Verdachtsfällen oder der Analyse von Datenschutz-Verstößen
- die regelmäßige sowie bei Bedarf ad hoc-Berichterstattung, insbesondere über Datenschutz-Risiken und Tätigkeiten
- auf Einladung Teilnahme an und Berichterstattung in den Sitzungen des Data Privacy Management Committees.

Der Fachbereich Data Privacy empfiehlt die Erstellung eines Datenschutz-Plans, der die Aufgaben des jeweiligen Datenschutz-Koordinators für das von ihm verantwortete datenschutz-relevante Themengebiet umfasst. Dieser wird in der Regel für ein Kalenderjahr erstellt und kann fortwährend aktualisiert werden. Der Fachbereich Data Privacy stellt hierfür eine Vorlage zur Verfügung.

Der Datenschutz-Koordinator kann einen Teil der Aufgaben an Mitarbeiter seines Fachbereichs delegieren. Damit die Datenschutz-Koordinatoren sowie ihn unterstützende Mitarbeiter ihren Aufgaben nachkommen können, werden sie vom Fachbereich Data Privacy entsprechend beraten und begleitet. Darüber hinaus erfordert die Rolle als Datenschutz-Koordinator und die Umsetzung der damit verbundenen Aufgaben insbesondere die folgenden Kompetenzen:

- ein uneingeschränktes Zugriffs- und Informationsrecht,
- Beratungskompetenz (inkl. dem Recht, verpflichtende Trainings bereitzustellen),
- ein Eskalationsrecht an die Geschäftsführung und
- ein Recht, Kontrollmaßnahmen durchzuführen

Die Geschäftsführung wird den Datenschutz-Koordinator in dokumentierter Form mit den oben aufgeführten Kompetenzen und erforderlichen Ressourcen ausstatten. Soweit bei einzelnen Aufgaben der Datenschutz-Koordinator durch einzelne Mitarbeiter unterstützt wird, werden die Kompetenzen auf diese ausgeweitet bzw. für diese eingerichtet.

Zur ordnungsgemäßen Erfüllung der Kernaufgaben nehmen sowohl die Datenschutz-Koordinatoren als auch Mitarbeiter, welche ihn bei seinen Aufgaben unterstützen, regelmäßig (in der Regel jährlich) an Fortbildungen teil. Die Auswahl über geeignete Fortbildungsmaßnahmen obliegt dem jeweiligen Datenschutz-Koordinator.

Es ist ein regelmäßiger Jour Fixe zwischen den Datenschutz-Koordinatoren und dem Fachbereich Data Privacy vorgesehen, um aktuelle Fragestellungen und Themen mit Datenschutz-Relevanz zu besprechen. Hierbei geht es insbesondere um den Austausch zu folgenden Themen:

- aktueller Status bzgl. Datenschutz-Risiken und ergriffener Maßnahmen,
- aktuelle Tätigkeiten/ Schwerpunkten sowie Erkenntnisse und
- rechtliche Änderungen

Der regelmäßige Austausch mit den Fachbereichen stellt einen bedeutenden Erfolgsfaktor zur Stärkung der Datenschutz-Kultur (wesentliches Element eines DPMS) bei Ottobock dar. Um diesen Austausch und die damit verbundene organisatorische Durchdringung von Datenschutz-Bewusstsein und -Kultur zu erreichen, werden dezentrale Datenschutz-Koordinatoren benannt.

Darüber hinaus soll hierdurch das Management von Datenschutz-Risiken auf eine breitere Basis gestellt werden. Die Festlegung der Fachbereiche, in denen Datenschutz-Koordinatoren benannt werden, erfolgt somit in einem ersten Schritt risikoorientiert für datenschutz-relevante Themengebiete (definiert als Teilbereiche, die wesentliche Datenschutz-Risiken beinhalten).

Weitere besondere Schnittstellen sind im Anhang angefügt.

9. Data Privacy Management Committee

Das Datenschutz-Management Committee [im Weiteren: DPMC] fungiert als zentrales Gremium der Datenschutz-Organisation und tagt quartalsweise. Unter dem Vorsitz des CXOs, ist ebenso der CFO fester Bestandteil des DPMCs. Das DPMC ist ein Beratungsgremium. Entscheidungen werden durch die Geschäftsführung getroffen und protokolliert.

Das DPMC besteht aus den folgenden ständigen Mitgliedern:

- CXO
- Head of Data Privacy
- Data Privacy Manager und weitere relevante Mitarbeiter des Fachbereichs Data Privacy

Einem Mitarbeiter des Fachbereichs Data Privacy obliegt die Führung eines Ergebnisprotokolls der Sitzung.

Der Betriebliche Datenschutzbeauftragte kann jederzeit als Gast an den Sitzungen des DPMC teilnehmen und jedes Mitglied kann seine Teilnahme anfordern.

Das DPMC kann weitere Gäste, wie etwa Regional Presidents oder Fachbereichsleiter, zu den Sitzungen einladen.

Zu den Kernaufgaben des DPMC gehören insbesondere die

- Aufsichtsfunktion:
  Über den im DPMC vertretenen geschäftsführenden Direktor übt die Geschäftsführung die Aufsicht über den Fachbereich Data Privacy aus
- Planungs- und Koordinationsfunktion:
  Austausch zu aktuellen und geplanten Aktivitäten inkl. Überwachungshandlungen
- Informationsfunktion:
  Vorstellung ausgewählter Datenschutz-Themen; insb. mit hohem Datenschutz-Risiko und Aufzeigen von Handlungsbedarf
- Entscheidungsvorbereitungsfunktion:
  Soweit Entscheidungen der Geschäftsführung mit einem Datenschutz-Bezug notwendig sind, werden diese durch das DPMC vorbereitet, bzw. durch die im DMPC anwesende Geschäftsführung direkt getroffen

E. DATENSCHUTZ-RISIKEN

Ottobock ist wie jedes Unternehmen unterschiedlichen Datenschutz-Risiken ausgesetzt. Datenschutz-Risiken sind die Risiken, die sich aus Verstößen gegen für

Ottobock verbindliche rechtliche Regelungen und Vorgaben sowie deren Konkretisierung im Rahmen von Ottobock-internen Regelwerken ergeben können. Eine nicht abschließende Liste möglicher Risiken ist im Anhang enthalten.

Verwirklichen sich Datenschutz-Risiken, so kann dies für Ottobock hohe Schäden wie z.B. Sanktionsschäden oder weitere finanzielle Schäden begründen. Darüber hinaus können auch persönliche Haftungsschäden der Organe sowie wesentliche Reputationsschäden Indikatoren für Datenschutz-Risiken darstellen.

Beim Management von Datenschutz-Risiken kommt den Fachbereichen eine zentrale Rolle zu. Je nach Tätigkeitsfeld gelten unterschiedliche rechtliche Regelungen und Vorgaben. Jeder Fachbereich ist damit einer spezifischen Datenschutz-Risikosituation ausgesetzt und ist dafür verantwortlich, die entsprechenden Datenschutz-Risiken zu kennen, zu steuern sowie zu minimieren.

F. INTERNE KOMMUNIKATION

1. Grundlegendes Kommunikationskonzept

Die Kommunikation des Fachbereichs Datenschutz- erfolgt nach dem nachfolgenden Kommunikationskonzept:

- Die Kommunikation mit den Fachbereichen erfolgt im Wesentlichen im Rahmen einer Beratung zu datenschutz-relevanten Vorgaben und konkreten Fragestellungen, insbesondere zu Themen mit DPMS-Bezug (inkl. Standards), (potenziellen) Datenschutz-Verdachtsfällen und dem datenschutzrelevanten Themengebiet Anti-Fraud und Anti-Korruption sowie in Bezug zu Auffälligkeiten im Rahmen von Überwachungshandlungen und entsprechendem Handlungsbedarf.
- Zudem werden durch den Fachbereich Data Privacy Mindeststandards und teilweise konkrete Vorgaben im Zusammenhang mit dem DPMS sowie weiterer Datenschutz-relevanter Sachverhalte im Rahmen von Richtlinien und weiteren schriftlich fixierten Vorgaben/Leitlinien (im Wesentlichen Code of Conduct, Richtlinie Anti-Korruption, Policy DPMS) sowie dem Intranet (z.B. Ansprechpartner, Beschreibung des DPMS und Verknüpfung zu relevanten Dokumenten) mitgeteilt.
- Der Fachbereich Data Privacy t ist im regelmäßigen Austausch mit den zu benennenden Datenschutz-Koordinatoren (in der Regel zwei Mal pro Jahr) und Ansprechpartnern der weiteren Fachbereiche, zu welchen wichtige Schnittstellen bestehen (vgl. hierzu Gliederungspunkt 6.4), wodurch der gegenseitige Informationsaustausch gewährleistet wird.
- Ein Austausch mit den weiteren Fachbereichen der zweiten (Verteidigungs-)Linie und der IKS-verantwortlichen Stelle erfolgt in der Regel quartalsweise (siehe Gliederungspunkt 3).

- Die Kommunikation mit der Geschäftsführung erfolgt neben den regelmäßigen Berichtswegen (siehe Gliederungspunkt 3) im Rahmen des Datenschutz-Management Committees (siehe Gliederungspunkt 9.) oder des regelmäßigen Jour Fixes.

Bei Bedarf (z.B. bei eintretenden Datenschutz-Vorfällen) erfolgen durch den Fachbereich Data Privacy ad-hoc Mitteilungen an relevante Fachbereiche bzw. an die Geschäftsführung. Eine nachhaltige Datenschutz-Kommunikation wird zudem durch, in der Regel anlassbezogene Verlautbarungen der Geschäftsführung sichergestellt (vgl. hierzu Gliederungspunkt 0.). Zudem werden die Unternehmenswerte und Datenschutz-Grundsätze in der Global Policy for Data Privacy und im Code of Conduct durch das persönliche Vorwort von Professor Hans Georg Näder, als Vorsitzender des Verwaltungsrats, unterstrichen.

2. Schulungen

Damit Datenschutz-Risiken frühzeitig erkannt und diesen sachgerecht begegnet werden kann, ist es unerlässlich allen Mitarbeitern die dafür notwendigen Kenntnisse zu vermitteln und in diesem Zusammenhang entsprechende Schulungen durchzuführen. Zur Vermittlung der notwendigen Kenntnisse erfolgen insbesondere:

- Datenschutz-Basisschulungen für neue Mitarbeiter,
- Durch den Fachbereich Data Privacy gesteuerte allgemeine Schulungsmaßnahmen zum Datenschutz
- Durch die Datenschutz-Koordinatoren gesteuerte ergänzende risikospezifische Datenschutz-Schulungen in den einzelnen Datenschutz Fokusthemen (vgl. hierzu Gliederungspunkt 2.).

Die Schulungsmaßnahmen finden entsprechende den Vorgaben des Art. 39 (1) lit b. DSGVO durch bzw. in Abstimmung mit dem Betrieblichen Datenschutzbeauftragten statt.
Um diesen Anforderungen gerecht zu werden, hat der betriebliche Datenschutzbeauftragte in Zusammenarbeit mit den Fachbereich Data Privacy und in Abstimmung mit dem Fachbereich HR, ein Datenschutz-Schulungskonzept zu erarbeiten. Es gibt einen einheitlichen Rahmen vor, in welchem die relevanten Schulungen je Datenschutz Fokusthema (vgl. hierzu Gliederungspunkt 2.) durchzuführen sind. Die Verantwortung für die Umsetzung des Schulungskonzepts sowie die Durchführung der Schulungen liegt bei den jeweiligen Fachbereichsleitern.

Der Fachbereich Data Privacy berät die Fachbereiche bei Bedarf im Rahmen der Umsetzung des Schulungskonzepts und führt, themenabhängig (z.B. Anti-Korruption), eigene Schulungen durch.

3. Interne Berichterstattung

Der Fachbereich Data Privacy informiert die Geschäftsführung in Textform über die Datenschutz-Aktivitäten des vergangenen Jahres und gibt einen Ausblick auf die Aktivitäten des kommenden Jahres. Der Jahresbericht ist der Geschäftsführung zu übergeben und durch diese dem Verwaltungsrat, dem Vorsitzenden des Aufsichtsrats sowie dem Prüfungsausschuss des Aufsichtsrats zur Kenntnisnahme weiterzuleiten.

Zudem berichtet der Fachbereich Data Privacy regelmäßig, in der Regel quartalsweise, über aktuelle Datenschutz-Themen im Management Board und im Rahmen der Sitzungen des DPMC (vgl. hierzu Gliederungspunkt 9.).

Je nach Sachverhalt kann außerhalb der regulären Berichterstattung ad-hoc an den CEO und/oder die gesamte Geschäftsführung berichtet werden.

Daneben berichtet der Fachbereich Data Privacy die Ergebnisse der Datenschutz-Risikoanalyse an den Fachbereich Corporate Risk Management, um eine konsolidierte Betrachtung der Gesamtrisikolage von Ottobock zu ermöglichen. Darüber hinaus findet ein Austausch zur Darstellung von Datenschutz-Risiken statt, um Inkonsistenzen in der Berichterstattung zu vermeiden.

Um seinen Berichtspflichten nachkommen zu können, erhält der Fachbereich Data Privacy von den für die Datenschutz Fokusthemen verantwortlichen Fachbereichen dezentrale Berichte.

4. Kommunikation mit Datenschutzbehörden

Die Kommunikation mit Datenschutzbehörden zu datenschutz-relevanten Sachverhalten erfolgt – sofern im Rahmen von Schnittstellenvereinbarungen nicht anders vereinbart – je nach Sachverhalt durch den Fachbereich Data Privacy (als Teilbereich von Cyber Security) unterstützt durch den Betriebliche Datenschutzbeauftragten.
Soweit Ordnungswidrigkeiten- und strafrechtliche Verfahren konkret drohen, kann der Behördenkontakt auch durch den Fachbereich Legal erfolgen. Legal hat hierüber ein Erstentscheidungsrecht. Dem Fachbereich Data Privacy Management ist in diesen Fällen – sofern für die Tätigkeit erforderlich – hierüber Bericht zu erstatten.

G. EXTERNE KOMMUNIKATION

1. Kommunikation mit Betroffenen

Die Kommunikation mit den Betroffenen zur Umsetzung von Betroffenenrecht obliegt dem externen Datenschutzbeauftragten unterstützt durch den Fachbereich Data Privacy.

2. Weitere externe Kommunikation

Bereitstellung von Informationen an Externe

Auf der Homepage von Ottobock werden Dritten datenschutz-relevante Informationen durch den Fachbereich Data Privacy zur Verfügung gestellt. Neben dem Code of Conduct wird z.B. auch auf die Hinweisgeberstelle von Ottobock hingewiesen.

Kommunikation gegenüber Lieferanten

Die allgemeinen Einkaufsbedingungen der Ottobock SE &Co. KGaA sehen eine Verpflichtung der Lieferanten auf bestimmte datenschutz-relevante Sachverhalte vor.

Kommunikation mit Staatsanwaltschaft, Polizei, LKA oder BKA (ggf. ausländische Strafverfolgungsbehörden)

Die Kommunikation mit o.g. Stellen zu datenschutz-relevanten Sachverhalten erfolgt stets über den Fachbereich Legal. Eine Einbindung des Fachbereichs Data Privacy, Datenschutz-Koordinatoren oder anderen betroffenen Fachbereichen erfolgt bei Bedarf je nach Sachverhalt.

Kommunikation externen Prüfern

Die Kommunikation externen Prüfern zu datenschutz-relevanten Sachverhalten erfolgt – sofern im Rahmen von Schnittstellenvereinbarungen nicht anders vereinbart – je nach Sachverhalt durch den Fachbereich Data Privacy (als Teilbereich von Cyber Security), Group Tax, Environment, Health and Safety, Compliance Treasury (für das Thema Geldwäscheprävention) oder Regulatory Affairs. Der Fachbereich Data Privacy ist im Vorfeld in die Kommunikation mit einzubinden.

Soweit Ordnungswidrigkeiten- und strafrechtliche Verfahren konkret drohen, erfolgt der Behördenkontakt durch den Fachbereich Legal (Hoheit bei Legal). Dem Fachbereich Data Privacy ist in diesen Fällen – sofern für die Tätigkeit erforderlich – hierüber Bericht zu erstatten.

Kommunikation mit der Presse

Sofern Datenschutz-Vorfälle oder andere datenschutz-relevante Sachverhalte eine Kommunikation mit Vertretern der Presse erforderlich machen, ist der Fachbereich Data Privacy Management im Vorfeld durch die Unternehmenskommunikation einzubinden, um die Inhalte zu prüfen und abzustimmen.

Kommunikation mit Verbänden und Arbeitskreisen

Die Kommunikation im Rahmen von Verbandsarbeit oder Arbeitskreisen obliegt grundsätzlich den Fachbereichen. Hinsichtlich datenschutz-relevanten Sachverhalten ist eine Einbindung des Fachbereichs Datenschutz-Management und je nach Sachverhalt ggf. Datenschutz-Koordinatoren im Vorfeld erforderlich.

H. DATENSCHUTZ-ÜBERWACHUNG UND ANPASSSUNG

Das DPMS befindet sich fortwährend in der Weiterentwicklung bzw. Optimierung, um eine laufende Anpassung an aktuelle Gegebenheiten (z.B. Eintritt in neue Märkte, neue rechtliche Vorgaben) zu ermöglichen und aus identifizierten Schwachstellen zu lernen und künftig zu vermeiden. Zur Identifizierung von potentiellen Schwachstellen wird das DPMS in regelmäßigen Abständen überwacht bzw. überprüft.

Ziel der Datenschutz-Überwachung ist es, die Angemessenheit und Wirksamkeit des DPMS als Ganzes zu beurteilen. Die Beurteilung ist von einer prozessunabhängigen Stelle, wie z.B. der Internen Revision oder externen Prüfern, durchzuführen. Darüber hinaus können auch die risikoorientierten Überwachungshandlungen Rückschlüsse auf die Angemessenheit und Wirksamkeit des DPMS geben. Es gilt hierbei zum einen festzustellen, ob sich die im Rahmen des DPMS implementierten Maßnahmen eignen, die damit verfolgte Zielsetzung, das Minimieren der Datenschutz-Risiken, zu erreichen und zum anderen, ob die Maßnahmen auch wirksam ausgestaltet sind; d.h. „gelebt werden“. Zudem ist auch zu untersuchen, ob die vorhandenen Maßnahmen ausreichen bzw. bestimmte risikoreduzierende Maßnahmen fehlen.

Die Überprüfung des DPMS ist in regelmäßigen Abständen durchzuführen. Sofern bei der Überprüfung des DPMS festgestellt wird, dass die im Rahmen des DPMS implementierten Maßnahmen nicht oder nur teilweise angemessen oder wirksam ausgestaltet sind oder Maßnahmen fehlen, ist ein entsprechend Handlungsbedarf abzuleiten.

Neben dem im Rahmen der Datenschutz-Überwachung identifizierten Verbesserungsbedarf werden insbesondere auch festgestellte Datenschutz-Verstöße als Anlass zur Überprüfung des DPMS genommen, um festzustellen, ob z.B. systematischem Fehlverhalten durch bestimmte Maßnahmen des DPMS entgegengewirkt werden kann. Sofern ein Datenschutz-Verstoß aufgedeckt wird, wird ein „Follow up-Prozess“ durch den Fachbereich Data Privacy Management angestoßen. Hierbei nehmen die betroffenen Fachbereiche eine Analyse der Ursachen für den Verstoß vor, etablieren Abhilfemaßnahmen und melden die Durchführung an den Fachbereich Data Privacy.

I. VERÖFFENTLICHUNGS- UND VERSIONIERUNGSHINWEIS

Die Policy Data Privacy Management System nebst Anhängen wird in elektronischer Form im Intranet der Ottobock SE & Co. KGaA und in der unternehmensweit verwendeten Business-Process-Management-Software hinterlegt.

Version	Datum	Autor	Anmerkungen
1.0	24-02-28	Matthias Horn	1. Version

Diese Policy wird regelmäßig (mindestens jährlich) hinsichtlich ihrer Aktualität überprüft und gegebenenfalls angepasst. Soweit unterjährig wesentliche rechtliche Änderungen in Kraft treten, welche Auswirkungen auf die hier beschriebenen Inhalte haben, erfolgt eine kurzfristige Überarbeitung dieser.

Herausgeber
Ottobock SE & Co. KGaA
Max-Näder-Str. 15
37115 Duderstadt, Deutschland

Ansprechpartner

Matthias Horn
Data Privacy Lawyer
E-Mail: privacy@ottobock.de

J. ANHÄNGE

Dieser Policy sind verschiedene Anhänge beigefügt. Die Anhänge können durch den Head of Data Privacy direkt abgeändert werden. Soweit hierbei die aufgeführten Organisationsvereinbarungen betroffen sind, können diese durch den Head of Data Privacy und den Leiter des betroffenen Fachbereichs einvernehmlich, jeweils in Abstimmung mit den für die Fachbereiche verantwortlichen geschäftsführenden Direktor, abgeändert werden.

- Schnittstellenvereinbarungen mit Fachbereichen der ersten (Verteidigungs-)Linie
- Schnittstellenvereinbarung der dritten (Verteidigungs-)Linie
- Übersicht Datenschutzrisiken
- Glossar

K. ANHANG ORGANISATIONSVEREINBARUNGEN MIT FACHBEREICHEN DER ERSTEN (VERTEIDIGUNGS-)LINIE

Neben dem Fachbereich Data Privacy tragen die Fachbereiche der ersten (Verteidigungs-)Linie die Verantwortung (siehe Gliederungspunkt 10) für unterschiedliche datenschutz-relevante Themengebiete (siehe Gliederungspunkt 8). Die Leiter dieser Bereiche benennen Datenschutz-Koordinatoren.

Datenschutz-Fokus-Thema	**Verantwortlicher Fachbereich**
Datenschutz im Beschäftigungsverhältnis	Global HR-Management (Leitung Global HR-Management)
Datenschutz in der Informationstechnik	Global IT (Leitung Global IT)
Datenschutz Patient Care	Patient Care (Leitung Patient Care)
Datenschutz in Forschung und Entwicklung	Global Research and Development (Leitung Research and Development)
Datenschutz in Clinical Research	Clinical Research (Leitung Clinical Research)
Datenschutz in der Marktforschung	Global O&P Solutions (Leitung Global O&P Solutions)
Datenschutz Marketing Technologies	Marketing-Technologies (Leitung Marketing Technologies)
Digital Health Solution	Digital Health Solution (Leitung Digital Health Solution als Teilbereich von Marketing-Solution)

I. Organisationsvereinbarung mit dem Global HR-Management

Die Leiter der Fachbereiche Data Privacy und Global HR-Management haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

II. Organisationsvereinbarung mit Global IT

Die Leiter der Fachbereiche Data Privacy und Global IT haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

III. Organisationsvereinbarung mit Patient Care

Die Leiter der Fachbereiche Data Privacy und Patient Care haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

IV. Organisationsvereinbarung mit Global Research and Development

Die Leiter der Fachbereiche Data Privacy und Global Research and Development haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

V. Organisationsvereinbarung mit Clinical Research

Die Leiter der Fachbereiche Data Privacy und Global Research and Development haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

VI. Organisationsvereinbarung mit O&P Solutions

Die Leiter der Fachbereiche Data Privacy und Global Research and Development haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

VII. Organisationsvereinbarung Marketing-Technologies

Die Leiter der Fachbereiche Data Privacy und Global Marketing-Technologies haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

VIII. Organisationsvereinbarung Digital Health Solution

Die Leiter der Fachbereiche Data Privacy und Digital Health Applications haben eine Organisationsvereinbarung entsprechend der Datenschutz-Organisation (Gliederungspunkt D.) vereinbart.

L. ANHANG SCHNITTSTELLENVEREINBARUNG MIT DER DRITTEN (VERTEIDIGUNGS-)LINIE

Berlin, März 2024

Schnittstellenvereinbarung Corporate Audit

Die Leiter der Fachbereiche Data Privacy und Corporate Audit haben folgende Schnittstellen gemeinsam definiert und vereinbart:

- Überprüfung der Angemessenheit und Wirksamkeit des implementierten DPMS im Rahmen von Revisionsprüfungen („Audits“) seitens Corporate Audit. Im Rahmen der Prüfung kann Audit best practice Hinweise erteilen und Datenschutz-Management kann Audit zu aufkommenden Fragestellungen und Prüfungsfeststellungen konsultieren.
- Prüfungsauftrag über die Tätigkeiten des Fachbereichs Data Privacy als zweite (Verteidigungs-)Linie. Im Rahmen der Prüfung kann Audit best practice Hinweise erteilen und Data Privacy kann Audit zu aufkommenden Fragestellungen und Prüfungsfeststellungen konsultieren.
- Regelmäßige datenschutz-relevante Audits, z.B. in operativen Fachbereichen
- Regelmäßiger Austausch:
  - im Rahmen der Erstellung des jährlichen Audit-Prüfungsplans und Datenschutz-Überwachungsplans, um z.B. zeitliche Überschneidungen zu vermeiden oder Synergien bei Vor-Ort-Prüfungen im Ausland zu nutzen,
  - zu datenschutz-relevanten Sachverhalten im Rahmen des CC; hierbei stehen insbesondere aktuellen risikorelevanten Sachverhalten und Entwicklungen im Fokus und
  - zur Schaffung einer konsistenten Berichterstattung gegenüber der Geschäftsführung zu datenschutz-relevanten Sachverhalten hinsichtlich Compliance-relevanter Themengebiete
- Zurverfügungstellung von Informationen seitens Corporate Audit bei Datenschutz-Sachverhalten wie der Identifizierung von (neuen) Datenschutz-Risiken im Rahmen von Revisionstätigkeiten; z.B.
  - Feststellungen im Rahmen der Prüfung datenschutz-relevanter Sachverhalte
  - Erkenntnisse/Informationen aus internen Untersuchungen (Investigations) mit Datenschutz-Bezug
- Zurverfügungstellung von Informationen seitens des Fachbereichs Data Privacy, sofern sich aus der Datenschutztätigkeit-Tätigkeit heraus revisionsrelevante Themen bzw. datenschutz-relevante Prüfungsthemen ergeben, z.B.
  - Neue rechtliche Anforderungen (und damit einhergehende Datenschutz-Risiken), welche nach der Umsetzung Gegenstand des Prüfungsplans sein sollten
  - Verdachtsfälle oder Hinweise auf Datenschutz-Vorfälle, welche im Rahmen einer internen Untersuchung (Investigation) näher analysiert und geprüft werden sollen (Quelle u.a. Hinweisgeberstelle), soweit die Investigation durch Corporate Audit durchgeführt wird
- Bearbeitung von Datenschutz-Vorfällen oder Datenschutz-Verdachtsfällen:
  - Die Bearbeitung von Datenschutz-Vorfällen oder Datenschutz-Verdachtsfällen liegt in der Hoheit des Fachbereichs Data Privacy.

- Sofern ein entsprechender Datenschutz-Vorfall vorliegt oder sich ein Anfangsverdacht bestätigt, kann der Fachbereich Data Privacy der Geschäftsführung empfehlen, die Durchführung von internen Untersuchungen durch den Fachbereich Corporate Audit oder durch Dritte (z.B. Wirtschaftsprüfungsgesellschaften) zu beauftragen
- Im Rahmen von externen Untersuchungen durch Behörden ist Data Privacy gemeinsam mit dem Betrieblichen Datenschutzbeauftragten bzw. Legal zuständig (Rechtsberatung)
- Die Kommunikation mit Behörden zu datenschutz-relevanten Sachverhalten obliegt je nach Sachverhalt dem Fachbereich Data Privacy, Legal, Regulatory Affairs, Group Tax, Treasury (für das Thema Geldwäscheprävention)
- Bei der Kommunikation zu datenschutz-relevanten Situationen mit der Presse o.ä. begleitet Data Privacy bzw. Legal.

***

M. ANHANG ZUM SCHULUNGSKONZEPT: MUSTERSCHULUNGSPLAN

Art:	Inhalt:	Fach-bereiche:	Schulungs-anlass	Zielgruppe:	Schulungs-methode:	Letzte Schulung	Turnus	Zeitpunkt
Basisschu-lung	Datenschutz	Alle Bereiche	Erstschulung	alle Mitarbei-ter	Online	Initial	jährlich	Q1

N. ANHANG DATENSCHUTZ-RISIKEN

Verstöße gegen formales Datenschutzrecht

- Fehlende bzw. nicht ausreichende Rechtsgrundlagen für die Verarbeitung von personenbezogenen, z.B. von Einwilligungen, Vertrag, gesetzliche Verpflichtung oder berechtigtes Interesse
- Fehlende Berücksichtigung der besonderen Anforderungen bei der Verarbeitung von Gesundheitsdaten (Art. 9 DSGVO)
- Fehlende Transparenz in Bezug auf Pflichtangaben /Datenschutzerklärung, Art, 12ff DSGVO
- Fehlende Einträge im Verarbeitungsverzeichnis, Art. 30 DSGVO
- Fehlende Vereinbarung zur Auftragsvereinbarung oder fehlende Vereinbarung bei Datenübermittlungen an Dienstleister und Partner
- Fehlende Garantien bei Drittstaatenübermittlungen
- Fehlende Meldung eines Data Breach i.S.d. Art. 33/34 DSGVO
- Fehlende Benennung von betrieblichen Datenschutzbeauftragten
- Fehlende Datenschutz-Folgenabschätzung

Verstöße gegen materielles Datenschutzrecht; Imagerisiken

- Verlust, unbeabsichtigte Löschung oder Kompromittierung von Patientendaten
- Besondere Risiken bestehen im Übrigen regelmäßig bei
    - Systemen, die große Mengen an Daten von Einzelpersonen verarbeiten (CRM-Systeme)
    - In der EU: Speicherung von personenbezogenen Daten in sog. Drittländern, d.h. in Ländern außerhalb von EU oder EWR. Das gleiche gilt, wenn von diesen Ländern der Zugriff auf personenbezogene Daten erfolgen kann, die in der EU gespeichert sind.

Grundsätze der Risiken im Datenschutz

- **Großes / kleines / ohne DSGVO-Bußgeld:** In Art. 83 Abs. 4 und 5 DSGVO werden zwei Bußgeldklassen für Verstöße gegen verschiedene Normen definiert.

  ➔ **Es können bis zu 4 % des weltweiten Jahresumsatzes verhängt werden!**

- Einige Verstöße sind gar nicht bußgeldbewehrt. Dies ist nicht nur wegen der Höhe eines möglichen Bußgeldes relevant, sondern auch, weil hierdurch auch die gesetzgeberische Wertung zum Ausdruck kommt, welche Verstöße besonders schwerwiegend und welche ggf. etwas weniger risikorelevant sind.

- **Imagerisiken:** Unabhängig von etwaigen Bußgeldrisiken sollte unbedingt berücksichtigt werden, welche Handlungen besondere Imagerisiken (auch in sozialen Medien) zur Folge haben können.

- **Normen mit / ohne Abwägung:** Bei Verstößen gegen Normen mit Abwägungsmöglichkeit (wie dem Vorliegen eines berechtigten Interesses i.S.d. Art. 6 Abs. 1 S. 1 (f) DSGVO oder der Angemessenheit von Schutzmaßnahmen) verbleibt häufig noch Argumentationsspielraum, so dass ein behaupteter Verstoß rechtlich nicht völlig eindeutig ist. Bei Normen ohne Abwägungsmöglichkeit (wie dem Vorliegen einer Einwilligung oder der Dokumentation des berechtigten Interesses) ist der Verstoß hingegen nicht bestreitbar und somit das Risiko noch höher.

- **Schadenersatzforderungen von Betroffenen:** Nach Art. 82 DSGVO kann jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter

- .**Schadenersatzforderungen von Vertragspartnern:** Aufgrund vertraglicher Verpflichtungen mit Bezug zum Datenschutz können Vertragspartner Schadenersatz geltend machen, soweit ein Verstoß gegen vertragliche Pflichten vorliegt.