Besitzer des Dokuments	Group CFO
Dokumentenhalter	Group CFO
Genehmigung	Verwaltungsrat der Bentley Endovascular Group AB (publ)
Datum der Genehmigung	2025-04-29

Data Privacy Policy

Bentley Endovascular Group AB (publ)

(Datenschutz-Richtlinie)

INHALT

1. Einleitung 3
2. Zweck 3
3. Anwendungsbereich 3
4. Grundsätze 3
5. Datenschutzbeauftragter 4
6. Rollen und Verantwortungsbereiche 4
7. Grundsätze für die Verarbeitung personenbezogener Daten 5
8. Rechtmäßigkeit der Datenverarbeitung 6
9. Aufbewahrungsfristen 7
10. Rechtmäßigkeit der Datenübermittlung 7
11. Datenverarbeitung im Auftrag von Bentley 7
12. Rechte der betroffenen Personen 8
13. Datenschutzkontrolle 10
14. Vertraulichkeit der Datenverarbeitung 10
15. Verletzungen des Schutzes personenbezogener Daten 10
16. Datenschutz-Folgenabschätzung 11
17. Untersuchungen 11
18. Verknüpfte Dokumente 11

1. EINLEITUNG

Die Bentley Endovascular Group AB (publ) (nachfolgend das „**Unternehmen**"; gemeinsam mit ihren Tochtergesellschaften nachfolgend auch „**Bentley**“, die „**Gruppe**" oder „**wir**") ist ein international tätiges Medizintechnikunternehmen mit Hauptsitz in Schweden und weltweiten Tochtergesellschaften.

Diese Richtlinie stellt Bentleys interne, verbindliche Regelung zur Erhebung, Verarbeitung, Übermittlung und Nutzung sämtlicher personenbezogener Daten dar. Sie dient dem Schutz personenbezogener Daten betroffener Personen und der Aufrechterhaltung eines angemessenen Schutzniveaus, indem sichergestellt wird, dass sämtliche datenschutzbezogenen Tätigkeiten mit den anwendbaren Datenschutzvorschriften – einschließlich der Europäischen Datenschutz-Grundverordnung („DSGVO“) sowie für die Schweizer Niederlassung von Bentley einschließlich des Schweizer Datenschutzgesetzes („DSG“) – in Einklang stehen.

2. ZWECK

Der Verwaltungsrat der Bentley Endovascular Group AB (publ) (im Folgenden das „**Board**“) hat diese Datenschutzrichtlinie (im Folgenden „**Richtlinie**“) beschlossen.

Der Zweck dieser Richtlinie besteht darin, die Einhaltung der Gesetze und Vorschriften zu gewährleisten, die für die Erhebung, Speicherung, Nutzung, Übermittlung, Weitergabe an Dritte und Aufbewahrung von persönlichen und sensiblen personenbezogenen Daten (in dieser Richtlinie auch als personenbezogene Daten bzw. sensible personenbezogene Daten bezeichnet) gelten.

3. ANWENDUNGSBEREICH

Diese Richtlinie gilt für alle unbefristet oder befristet beschäftigten Mitarbeitenden des Unternehmens (einschließlich etwaiger Vermittler, Tochtergesellschaften oder verbundenen Unternehmen). Sie gilt ebenso für jede natürliche oder juristische Person, die mit dem Unternehmen in Verbindung steht oder Funktionen im Zusammenhang mit dem Unternehmen oder in dessen Namen bzw. Auftrag ausübt. Dazu zählen unter anderem Mitglieder des Boards, Zeitarbeitskräfte, Aushilfen, Auftragnehmer, Berater und Lieferanten. Alle Mitarbeitenden und verbundenen Personen haben die in dieser Richtlinie dargelegten Grundsätze zu befolgen.

4. GRUNDSÄTZE

4.1 Die letztliche Verantwortung für diese Richtlinie liegt beim Board, die operative Zuständigkeit wird aber vom Group CFO wahrgenommen, der auch Dokumentenhalter ist. Die Richtlinie ist mindestens einmal jährlich auf notwendige Aktualisierungen zu überprüfen. Da sich Bentleys Geschäftstätigkeit und die regulatorischen Anforderungen laufend verändern, ist es von zentraler Bedeutung, dass der Group CFO sicherstellt, dass diese Richtlinie sowie die dazugehörigen Anweisungen regelmäßig aktualisiert werden. Der Group CFO ist für die ordnungsgemäße Dokumentation sämtlicher Änderungen dieser Richtlinie verantwortlich.

4.2 Diese Richtlinie ist in sämtlichen Angelegenheiten, die den Umgang mit personenbezogenen Daten natürlicher oder juristischer Personen betreffen – insbesondere bei der Erhebung, Verarbeitung und Übermittlung von Daten – zu beachten. Sie gilt nicht für anonymisierte Daten, sondern für sämtliche Mitarbeitenden, Auftragnehmer und Führungskräfte von

Bentley persönlich. Die Einhaltung dieser Richtlinie obliegt sowohl Bentley als auch den von ihr betroffenen Personen. Sie wird durch das Management von Bentley umgesetzt und ist für alle, auf die sie Anwendung findet, verbindlich. Sie ergänzt, ersetzt jedoch nicht bestehende nationale Datenschutzvorschriften. Gesetzliche Verpflichtungen bleiben durch diese Richtlinie unberührt. Im Falle eines Widerspruchs oder einer Unvereinbarkeit zwischen gesetzlichen Vorgaben und dieser Richtlinie gehen die gesetzlichen Bestimmungen vor. Die Regelungen dieser Richtlinie sind auch dann bindend, wenn es keine entsprechenden gesetzlichen Datenschutzvorgaben gibt. Vorgesetzte sind dafür verantwortlich, dass alle neu eingestellten Mitarbeitenden und Berater über diese Richtlinie informiert werden.

5. DATENSCHUTZBEAUFTRAGTER

Der Group CFO bestellt für Bentley eine(n) oder mehrere Datenschutzbeauftragte (im Folgenden „**DSB**“) gemäß den jeweils geltenden gesetzlichen Vorgaben. Der DSB wird bei der Ausübung seiner Aufgaben uneingeschränkt von der Geschäftsleitung von Bentley unterstützt. Der DSB ist dafür verantwortlich, die Einhaltung gesetzlicher Datenschutzvorschriften sowie der Bestimmungen dieser Richtlinie sicherzustellen. Der DSB berät die Geschäftsleitung von Bentley hinsichtlich der Erfüllung der datenschutzrechtlichen Pflichten des Unternehmens, überwacht die Einhaltung gesetzlicher Anforderungen sowie etwaiger Risiken und ist zuständig für die Kommunikation mit den Aufsichtsbehörden. Im Übrigen handelt der DSB gewissenhaft, entsprechend seiner fachlichen Qualifikation und ist weisungsfrei. Der DSB kann jederzeit bei Beschwerden, Auskunftsersuchen oder sonstigen datenschutzbezogenen Anliegen vertraulich kontaktiert werden. Die Kontaktaufnahme mit dem DSB ist wie folgt möglich: Datenschutz_BI@bentley.global.

6. ROLLEN UND VERANTWORTUNGSBEREICHE

Rolle	Verantwortungsbereich
Board	• Genehmigt die Richtlinie.
Group CEO	• Trägt die Verantwortung für die Strategie und eskalierten Anliegen des Group CFO.
Group CFO	• Gesamtverantwortung für die Richtlinie und die zugehörigen Anweisungen (Dokumentenhalter). • Führt regelmäßige Bewertungen zur Umsetzung durch und unterstützt Unternehmensbereiche bei der Entwicklung basierend auf Geschäftsanforderungen und Risiken. • Verantwortlich für die Aktualisierung der Richtlinie und deren Dokumentation (als Dokumentenhalter). • Genehmigt gruppenweite Richtlinien und Anweisungen gemäß dieser Richtlinie, falls notwendig. • Berichtet an Group CEO und Board.

IT Manager/Head of IT	• Verantwortlich für die Umsetzung der technischen und organisatorischen Maßnahmen zur Einhaltung der DSGVO. • Stellt sicher, dass Bentley stets ein aktuelles Verzeichnis der Verarbeitungstätigkeiten über personenbezogene Daten gemäß Art. 30 DSGVO führt. • Berichtet an den Group CFO.
DSB	• Gesamtverantwortung für die Einhaltung und Umsetzung der Datenschutzvorgaben. • Interne und externe Ansprechperson für datenschutzbezogene Anfragen und Vorfälle. • Zusammenarbeit mit der Aufsichtsbehörde, z. B. bei Kontrollmaßnahmen. • Bearbeitung von Meldungen und Anfragen gemäß dieser Richtlinie. • Meldet Risikobewertungen, Umsetzungsstände und besondere Hochrisikosachverhalte an den Group CFO. • Stellt Schulungsunterlagen für Mitarbeitende zur Verfügung. • Berichtet an den Group CFO.
Mitarbeitende, Vertragspartner und externe Parteien	• Alle Mitarbeitenden, Vertragspartner und externe Parteien sind zur Einhaltung dieser Richtlinie verpflichtet.

7. GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Bei der Verarbeitung personenbezogener Daten sind folgende Rechtsgrundsätze zu beachten:

7.1 Rechtmäßigkeit, Fairness und Transparenz: Die Erhebung personenbezogener Daten erfolgt auf rechtmäßige, faire und für die betroffene Person nachvollziehbare Weise. Die betroffene Person ist über die Verarbeitung sowie deren Zweck, den Verantwortlichen und etwaige Empfänger zu informieren.

7.2 Zweckbindung: Die Verwendung personenbezogener Daten muss einem zuvor festgelegten, eindeutigen und rechtmäßigen Zweck dienen und darf nicht in einer Weise erfolgen, die mit diesem Zweck unvereinbar ist. Spätere Zweckänderungen sind nur in Ausnahmefällen zulässig und bedürfen einer Begründung.

7.3 Datenminimierung, Speicherbegrenzung: Vor der Verarbeitung personenbezogener Daten ist stets zu prüfen, ob und inwieweit der Zweck der Verarbeitung mit dem vorgesehenen Ansatz erreicht werden kann. Wenn der Zweck auch ohne Rückgriff auf personenbezogene Daten erreicht werden kann, z.B. durch anonymisierte oder pseudonymisierte Daten, ist dieser

mildere Ansatz zu bevorzugen. Vorbehaltlich anderer behördlicher Vorschriften ist die Speicherung personenbezogener Daten für sachfremde oder zukünftige Zwecke unzulässig. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Zweck der Verarbeitung erforderlich ist. Sobald die gesetzlichen oder betrieblichen Aufbewahrungsfristen abgelaufen sind, müssen personenbezogene Daten gelöscht werden.

7.4 Richtigkeit: Die Richtigkeit, Vollständigkeit und Aktualität der erhobenen personenbezogenen Daten sind zu gewährleisten. Andernfalls sind unrichtige, unvollständige und nicht mehr aktuelle Daten unverzüglich zu berichtigen, zu ergänzen, zu aktualisieren oder zu löschen.

7.5 Integrität, Vertraulichkeit: Personenbezogene Daten sind vertraulich zu behandeln, und es sind geeignete technische und organisatorische Maßnahmen zu treffen, um einen angemessenen Schutz gegen unbefugte oder unrechtmäßige Verarbeitung und gegen unbeabsichtigten Verlust, Zerstörung oder Beschädigung zu gewährleisten.

7.6 Rechenschaftspflicht: Gemäß Artikel 30 der DSGVO führt das Unternehmen ein Verzeichnis aller Datenverarbeitungsaktivitäten, insbesondere um die Einhaltung der in dieser Richtlinie dargelegten Grundsätze nachzuweisen.

8. RECHTMÄSSIGKEIT DER DATENVERARBEITUNG

Nach den geltenden Datenschutzvorschriften ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn mindestens eine der folgenden Rechtsgrundlagen vorliegt:

8.1 Einwilligung in die Datenverarbeitung: Die betroffene Person kann ihre Einwilligung insbesondere zur Verarbeitung personenbezogener Daten zu Werbezwecken geben. Eine gültige Einwilligung muss freiwillig, konkret, in Kenntnis der Sachlage und unmissverständlich erteilt werden. Die betroffene Person muss vor der Erteilung der Einwilligung umfassend informiert werden. Die Einwilligungserklärung muss freiwillig sein und in der Regel schriftlich oder elektronisch abgegeben werden. Die Einwilligung muss ordnungsgemäß dokumentiert werden. Die betroffene Person muss außerdem die Möglichkeit haben, ihre Einwilligung jederzeit zu widerrufen. Wird die Einwilligung z. B. in die Verarbeitung personenbezogener Daten zu Werbezwecken widerrufen, dürfen Sie die betreffenden personenbezogenen Daten nicht zu Werbezwecken nutzen.

8.2 Datenverarbeitung auf der Grundlage vertraglicher Beziehungen: Die Verarbeitung ist zulässig, soweit sie für die Begründung, Durchführung, Beendigung oder Erfüllung eines bestehenden Vertrags erforderlich ist oder die Verarbeitung für die Durchführung oder Umsetzung vorvertraglicher Maßnahmen oder einer rechtlichen Verpflichtung des für die Verarbeitung Verantwortlichen erforderlich ist.

8.3 Die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen: Die Verarbeitung ist zulässig, soweit sie zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

8.4 Datenverarbeitung auf der Grundlage des berechtigten Interesses des für die Verarbeitung Verantwortlichen: Die Verarbeitung ist zulässig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und -freiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dies ist vor jeder Verarbeitung sorgfältig zu prüfen.

8.5 Rechtliche Verpflichtung zur Verarbeitung personenbezogener Daten: Die Verarbeitung ist zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Ein gängiges Beispiel ist die Verarbeitung personenbezogener Daten für Buchhaltungszwecke.

8.6 Verarbeitung besonderer Kategorien von personenbezogenen Daten: Besondere Kategorien personenbezogener Daten (zum Beispiel personenbezogene Daten über Gesundheit, ethnische Herkunft oder religiöse Überzeugungen) dürfen grundsätzlich nicht verarbeitet werden. Besondere Kategorien personenbezogener Daten dürfen jedoch verarbeitet werden, wenn z. B. die ausdrückliche Einwilligung der betroffenen Person vorliegt oder wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gegenüber der betroffenen Person erforderlich ist.

8.7 Werden personenbezogene Daten auf Websites oder in Apps oder mittels Cookies verarbeitet, erhoben oder genutzt, besteht stets die Pflicht, die betroffene Person durch Hinweise in leicht erkennbarer, unmittelbar zugänglicher und ständig verfügbarer Form darüber zu informieren. Für die Verwendung nicht wesentlicher Cookies wie Statistik-Cookies oder Marketing-Cookies ist eine gültige Einwilligung der betroffenen Person (frei, spezifisch, in Kenntnis der Sachlage und unmissverständlich) erforderlich. Gleiches gilt für das Profiling, also die Erstellung von Nutzungsprofilen zur Auswertung des Internetnutzungsverhaltens. Das Profiling ist nur auf der Grundlage einer gesetzlichen Erlaubnis oder der Zustimmung der betroffenen Person zulässig.

9. AUFBEWAHRUNGSFRISTEN

Eine grundlegende Anforderung der DSGVO ist, dass personenbezogene Daten nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden dürfen, die die Identifizierung von Personen ermöglicht. Jede Organisation innerhalb von Bentley und ihre Mitarbeitenden sind dafür verantwortlich, personenbezogene Daten nicht länger als nötig zu verarbeiten und alle zusätzlichen Verfahren und Dokumente einzuhalten, die von Bentley in Bezug auf die Aufbewahrungsfristen angenommen wurden.

10. RECHTMÄSSIGKEIT DER DATENÜBERMITTLUNG

Eine Übermittlung personenbezogener Daten an Dritte ist nur unter den Bedingungen dieser Richtlinie für eine rechtmäßige Datenverarbeitung zulässig. Folglich ist eine Übermittlung nur dann rechtmäßig, wenn sie gesetzlich zulässig ist und einem bestimmten Zweck dient. Wenn personenbezogene Daten in ein Drittland außerhalb der EU/des EWR übermittelt werden sollen, müssen geeignete Schutzmaßnahmen getroffen werden.

11. DATENVERARBEITUNG IM AUFTRAG VON BENTLEY

11.1 Wenn eine externe natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle personenbezogene Daten im Auftrag von Bentley als Auftragsverarbeiter verarbeitet, muss mit dieser externen Stelle ein schriftlicher Datenverarbeitungsvertrag mit dem im geltenden Recht vorgeschriebenen Inhalt geschlossen werden (Artikel 28 der DSGVO). Die Datenverarbeitung muss gemäß den spezifischen Anweisungen des für die Verarbeitung Verantwortlichen (d. h. der betreffenden Bentley-Gesellschaft) durchgeführt werden.

11.2 Der für die Verarbeitung Verantwortliche ist für die rechtskonforme Durchführung und Umsetzung der Verarbeitung verantwortlich. Er wählt den Auftragsverarbeiter sorgfältig aus, insbesondere nach der fachlichen Eignung, der Qualität seiner technisch-organisatorischen Datensicherheitsstandards oder vergleichbaren Indikatoren für die Zuverlässigkeit.

11.3 Der für die Verarbeitung Verantwortliche gewährleistet ein Höchstmaß an Datenschutz für den Auftragsverarbeiter, indem er Anweisungen erteilt, z. B. in Bezug auf Datensicherheitsmaßnahmen, Verantwortlichkeiten und Rechenschaftspflichten zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen.

12. RECHTE DER BETROFFENEN PERSONEN

Die betroffenen Personen können die folgenden Datenschutzrechte ausüben, sofern die sachlichen Voraussetzungen der jeweiligen Rechte erfüllt sind:

12.1 Recht auf Information: Jede betroffene Person hat das Recht, Auskunft darüber zu verlangen, ob personenbezogene Daten, die sie betreffen, im Unternehmen verarbeitet werden und wenn ja, welche Daten zu welchem Zweck, aus welcher Quelle und wie lange gespeichert werden. Im Falle der Weitergabe von Daten an Dritte muss auch Auskunft über die Identität des Empfängers und die Kategorien von Empfängern erteilt werden.

Bevor der für die Verarbeitung Verantwortliche die Informationen zur Verfügung stellt oder auf ein anderes Ersuchen der betroffenen Person antwortet, stellt er die Identität der betroffenen Person fest und ergreift erforderlichenfalls Maßnahmen, um etwaige Zweifel an der Identität der anfragenden Person zu beseitigen.

12.2 Recht auf Auskunft: Jede betroffene Person hat das Recht, eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten im Unternehmen verarbeitet werden, und wenn ja, Informationen darüber zu erhalten, wie das Unternehmen die personenbezogenen Daten verarbeitet, sowie eine Kopie der personenbezogenen Daten zu erhalten.

12.3 Recht auf Berichtigung: Jede betroffene Person kann die unverzügliche Berichtigung oder Vervollständigung der sie betreffenden unrichtigen oder unvollständigen personenbezogenen Daten verlangen.

12.4 Recht auf Löschung ("Recht auf Vergessenwerden"): Jede betroffene Person hat das Recht auf unverzügliche Löschung der sie betreffenden personenbezogenen Daten, sobald einer der folgenden Gründe für die Löschung vorliegt:

- Der Zweck der Datenverarbeitung ist nicht oder nicht mehr gegeben.
- Eine Rechtsgrundlage für die Datenverarbeitung fehlt oder ist weggefallen, da die betroffene Person ihre Einwilligung widerrufen hat.
- Die betroffene Person legt Widerspruch gegen die Datenverarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten werden zu Zwecken des Direktmarketings verarbeitet und die betroffene Person widerspricht der Verarbeitung.
- Die Datenverarbeitung ist unrechtmäßig.
- Die Verarbeitung personenbezogener Daten ist nicht (mehr) zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.
- Wurden personenbezogene Daten veröffentlicht und besteht eine Verpflichtung zu

ihrer Löschung, müssen weitere verantwortliche Stellen darüber informiert werden, dass die betroffene Person sie aufgefordert hat, alle Verknüpfungen zu den betreffenden personenbezogenen Daten oder Kopien oder Duplikate davon zu löschen.

12.5 Recht auf Einschränkung der Verarbeitung: Die betroffene Person hat das Recht, die Verarbeitung der sie betreffenden personenbezogenen Daten einzuschränken, sobald einer der nachstehenden Gründe vorliegt:

- Die betroffene Person bestreitet die Richtigkeit der personenbezogenen Daten. Eine Einschränkung wird für den Zeitraum vorgenommen, in dem der Verantwortliche die Richtigkeit überprüft
- Die Datenverarbeitung ist unrechtmäßig, aber die betroffene Person verlangt die Einschränkung der Nutzung anstelle der Löschung der personenbezogenen Daten.
- Die personenbezogenen Daten werden von dem für die Verarbeitung Verantwortlichen nicht mehr für die Zwecke der Verarbeitung benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt. Die Einschränkung erfolgt für den Zeitraum, in dem der für die Verarbeitung Verantwortliche den Widerspruch prüft.

Nach einer wirksamen Einschränkung der Verarbeitung dürfen die betreffenden personenbezogenen Daten nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer oder auf der Grundlage eines wichtigen öffentlichen Interesses verarbeitet werden. Die betroffene Person ist über die Aufhebung der Einschränkung zu unterrichten.

12.6 Recht auf Datenübertragbarkeit: Beruht die Datenverarbeitung auf einer Einwilligung oder ist sie für die Erfüllung eines Vertrags erforderlich, hat die betroffene Person das Recht, die personenbezogenen Daten, die sie dem Unternehmen zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format an einen anderen Verantwortlichen zu übermitteln, soweit dies technisch möglich ist.

12.7 Recht auf Widerspruch: Jede betroffene Person hat das Recht, einer Datenverarbeitung, die auf einer Einwilligung beruht oder zur Wahrung berechtigter Interessen erforderlich ist, jederzeit zu widersprechen. Dazu muss das Ergebnis einer Abwägung ergeben, dass das schutzwürdige Interesse der betroffenen Person, das sich aus einer besonderen Situation ergibt, das Interesse des Unternehmens an der Verarbeitung überwiegt. Ein Widerspruchsrecht besteht nicht, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

12.8 Recht auf Beschwerde: Darüber hinaus hat jede betroffene Person das Recht, sich bei der zuständigen Aufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten unrechtmäßig erfolgt ist.

Um ein Recht auf Datenschutz auszuüben, kann sich die betroffene Person an den DSB wenden. Der Antrag der betroffenen Person wird unverzüglich, spätestens jedoch einen Monat nach Eingang des Antrags beim Unternehmen, geprüft und bearbeitet. Jede/r Mitarbeitende ist daher dafür verantwortlich, jeden Antrag der betroffenen Person, von dem er/sie Kenntnis erlangt, seinem Vorgesetzten und dem DSB zu melden. Der DSB ist dann für die Untersuchung und Bearbeitung des Antrags zuständig, wobei er von anderen

Mitarbeitenden unterstützt wird.

13. DATENSCHUTZKONTROLLE

13.1 Um ein angemessenes Schutzniveau und die Einhaltung der geltenden Datenschutzvorschriften zu gewährleisten, muss der DSB die Einhaltung dieser Politik regelmäßig durch Audits und andere Kontrollmechanismen überwachen.

13.2 Die Ergebnisse jedes Audits sind zu dokumentieren und dem IT-Manager/Head of IT und dem Group CFO zu melden. Ein Datenschutzaudit ist erfolgreich abgeschlossen, wenn alle dokumentierten Mängel durch die Umsetzung geeigneter Maßnahmen behoben wurden. Dies ist entsprechend zu überprüfen.

14. VERTRAULICHKEIT DER DATENVERARBEITUNG

14.1 Alle Mitarbeitenden sind auf die Einhaltung des Datenschutzes (Datengeheimnis) verpflichtet. Den Mitarbeitenden ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Handelt ein/e Mitarbeitende/r unbefugt, z. B. wenn er in Ausübung seiner Tätigkeit personenbezogene Daten verarbeitet, ohne dazu angewiesen oder befugt zu sein, kann er mit einem Disziplinarverfahren rechnen.

14.2 Alle Mitarbeitenden müssen vor Aufnahme ihrer Tätigkeit eine Vertraulichkeitserklärung unterzeichnen. Sie müssen sicherstellen, dass die im Rahmen ihrer Tätigkeit gewonnenen personenbezogenen Daten nicht für private oder wirtschaftliche Interessen verwendet, an Unbefugte weitergegeben oder in sonstiger Weise zugänglich gemacht werden. Diese Verpflichtung gilt auch nach Beendigung des Arbeitsverhältnisses. Bei Aufnahme des Arbeitsverhältnisses wird der Arbeitnehmer über seine Verschwiegenheitspflicht belehrt und schriftlich dazu verpflichtet. Um ein hohes Maß an Vertraulichkeit zu gewährleisten, dürfen die Mitarbeitenden nur in dem Umfang Zugang zu personenbezogenen Daten erhalten, wie es für die Erfüllung ihrer Aufgaben konkret erforderlich ist (Need-to-know-Prinzip). Es ist ein detailliertes und vollständiges Berechtigungskonzept/Richtlinie/Anweisungen zu erstellen und sorgfältig zu pflegen, das den Mitarbeitenden entsprechend ihrer Rolle und Verantwortung definierte Zugriffsberechtigungen/Rechte einräumt.

15. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

15.1 Eine "**Verletzung des Schutzes personenbezogener Daten**" ist eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Zerstörung, Verlust, Änderung, unbefugten Offenlegung oder zum Zugriff auf personenbezogene Daten führt, die übermittelt, gespeichert oder anderweitig verarbeitet werden. Übliche Beispiele für Verletzungen des Schutzes personenbezogener Daten sind das Hacken eines Servers oder der Diebstahl eines Computers mit personenbezogenen Daten.

15.2 Sowohl die für die Verarbeitung Verantwortlichen als auch die Auftragsverarbeiter haben nach der DSGVO im Falle einer Verletzung des Schutzes personenbezogener Daten Verpflichtungen. Im Wesentlichen ist der für die Verarbeitung Verantwortliche dafür verantwortlich, die zuständige Aufsichtsbehörde spätestens 72 Stunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen und die von der Verletzung betroffenen Personen unverzüglich zu informieren. Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen unverzüglich nach Bekanntwerden eines Verstoßes gegen den Schutz personenbezogener Daten informieren.

15.3 Im Falle einer Verletzung des Schutzes personenbezogener Daten, eines Verstoßes gegen diese Richtlinie oder gegen andere Vorschriften zum Schutz personenbezogener Daten muss der/die verantwortliche Mitarbeitende die Datenverletzung unverzüglich seinem/ihrer Vorgesetzten und dem DSB melden. Die Meldung muss alle Informationen enthalten, die zur Feststellung des Sachverhalts erforderlich sind, insbesondere den Empfänger, die spezifischen personenbezogenen Daten, die betroffen sind, sowie die Art und den Umfang der von dem Vorfall betroffenen Daten. Jede/r Mitarbeitende ist dafür verantwortlich, jede Verletzung des Schutzes personenbezogener Daten, von der er Kenntnis erhält, seinem Vorgesetzten/Manager und dem DSB zu melden. Der DSB ist dann für die Untersuchung und den Umgang mit der Verletzung verantwortlich, wobei er von anderen Mitarbeitenden unterstützt wird.

15.4 Besteht für die jeweilige Datenschutzverletzung eine Meldepflicht gegenüber den Aufsichtsbehörden, so kommt der DSB dieser Pflicht unverzüglich nach. Wurde eine Datenschutzverletzung, ein Verstoß gegen diese Richtlinie oder ein Verstoß gegen andere Datenschutzvorschriften fahrlässig oder vorsätzlich herbeigeführt, kann dies arbeitsrechtliche Konsequenzen nach sich ziehen. Darüber hinaus kommen straf- und zivilrechtliche Sanktionen in Betracht, wie etwa die Geltendmachung von Schadensersatzansprüchen.

16. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wenn eine Form der Verarbeitung personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt, ist jede datenverarbeitende Abteilung verpflichtet, im Voraus eine Datenschutz-Folgenabschätzung für die geplante Datenverarbeitung durchzuführen. Für die Durchführung von Datenschutz-Folgenabschätzungen ist der DSB zuständig, der dabei von anderen Mitarbeitenden unterstützt wird.

17. UNTERSUCHUNGEN

17.1 Bei allen unternehmensinternen Untersuchungen müssen die geltenden Datenschutznormen und -pflichten eingehalten werden. Die Datenverarbeitung im Zusammenhang mit der Untersuchung muss in einem angemessenen Verhältnis zum Ziel der Untersuchung und zu den zu schützenden Interessen der Betroffenen stehen, d.h. geeignet, erforderlich und angemessen sein. Zu den unternehmensinternen Ermittlungen gehören Maßnahmen, die der Verhinderung, Aufklärung oder Feststellung einer schwerwiegenden arbeitsrechtlichen Pflichtverletzung oder einer Straftat dienen.

17.2 Stellen Sie sicher, dass der DSB einbezogen und zu Form, Umfang und anderen Einzelheiten aller Ermittlungsmaßnahmen konsultiert wird.

17.3 Die betroffene Person wird unverzüglich davon unterrichtet, dass gegen sie ermittelt wird und welche Maßnahmen getroffen werden.

18. VERKNÜPFTE DOKUMENTE

- Information Security Policy
- IT-Policy
- Business Continuity Policy

* * * *