**Datenschutzhandbuch**

1. Präambel
2. Zweck des Dokuments
3. Datenschutzgrundsätze
   1. Rechtmäßigkeit
   2. Verarbeitung nach Treu und Glauben
   3. Transparenz
   4. Zweckbindung
   5. Datenminimierung
   6. Richtigkeit
   7. Nachvollziehbarkeit
   8. Revisionsfähigkeit
   9. Speicherbegrenzung
   10. Integrität und Vertraulichkeit
   11. Rechenschaftspflicht
4. Datenschutzorganisation
   1. Bestellung eines betrieblichen Datenschutzbeauftragten
      1. Organisatorische Einrichtung im Unternehmen
      2. Aufgaben des Datenschutzbeauftragten
      3. Informations- und Informationszugangsrechte des Datenschutzbeauftragten
      4. Datenschutzberichte
   2. Konzernübergreifende Datenschutzorganisation, Konzerndatenschutzbeauftragter
   3. Datenschutz und Betriebsrat
5. Datenschutzmanagement
   1. Integration des Datenschutzmanagements in das Unternehmensmanagement
   2. Qualitätsmanagement
      1. Verankerung des Datenschutzes in den QM-Dokumenten
      2. Integration des Datenschutzes in den PDCA-Zyklus/Kontinuierlichen Verbesserungsprozess
      3. Integration des Datenschutzes in das Auditwesen
6. Datensicherheitsmanagement
   1. Integration des Datensicherheitsmanagements in das Informations- und IT-Sicherheitsmanagement
      1. Bestehende Normen und Zertifikate
      2. Berücksichtigung des Datenschutzes in den Maßnahmenzielen und Maßnahmen
      3. Informationsklassifizierung
      4. Definition der Datenschutzanforderungen der beteiligten Parteien
      5. Technische und organisatorische Maßnahmen zum Informations- und Datenschutz
7. Schutzziele und Schutzgrade der Daten, Vertraulichkeitsrichtlinie
8. Datenschutzdokumente
   1. Prozess- und Verfahrensübersicht
      1. Prozessübersicht personalbezogene Prozesse
      2. Prozessübersicht Kunden-/Lieferantenprozesse
      3. Allgemeine Prozesse
   2. Verzeichnis über die Verarbeitungstätigkeiten
      1. Übersicht über die Datenverarbeitungsverfahren und gemeinsame Angaben
      2. Beschreibung der einzelnen Verfahren
      3. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
   3. Risikobewertung und Verfahren zur Klassifizierung der personenbezogenen Daten nach Risikostufen und Schutzbedarfsfeststellung
   4. Checklisten und Dokumentationen über die Erhebungen des Datenschutzbeauftragten zum Datenschutz und zur Datensicherheit und Bewertung des Standes des Datenschutzes und der technischen und organisatorischen Maßnahmen
   5. Verantwortlichkeit für die Führung der Datenschutzdokumentation
9. Datenschutzprozesse und Verfahren

1. Recht der Betroffenen
2. Information der Betroffenen bei der Datenerhebung
3. Meldung von Datenschutzverletzungen
4. Datenschutz durch Technikgestaltung
   1. Beschaffung von Software
   2. Softwareentwicklung
   3. Implementation von Datenverarbeitungsverfahren
5. Datenschutzfolgenabschätzung und vorherige Konsultation der Aufsichtsbehörde gem. Art. 35 u. 36 DSGVO
6. Vertraulichkeit und Geheimhaltungspflichten
7. Datenverarbeitung im Auftrag
   1. Auswahl der Auftragnehmer
   2. Verträge über eine Datenverarbeitung im Auftrag
   3. Übersicht über Beauftragungen (Vertragsverzeichnis)
8. Gemeinsam Verantwortliche
   1. Verfahren und vertragliche Regelungen
9. Datenübermittlungen im Konzern und in Drittstaaten
   1. Konzerninterne Übermittlungen
   2. Übermittlung in Drittstaaten und Vertragsgrundlagen
10. Zusammenarbeit mit der Aufsichtsbehörde
11. Pflege und Versionisierung der Datenschutzdokumente
12. Nachweis der Einhaltung der DSGVO
    * + 1. **Präambel**

*(Beispieltext)*

Der Schutz von personenbezogenen Daten rückt zunehmend in den Fokus der betroffenen Personen, der Öffentlichkeit und der Gesellschaft. Dem trägt auch die Europäische Datenschutzgrundverordnung (DSGVO) Rechnung. Der Schutz von personenbezogenen Daten und Informationen (und ein großer Teil davon sind personenbezogene Daten) ist auch ein bedeutender Wirtschaftsfaktor und als solcher für unser Unternehmen von großer Bedeutung. Andererseits kann ein Missbrauch der Daten und Informationen nicht nur die Wirtschaftstätigkeit unseres Unternehmens und die betriebliche Funktion schwer beeinträchtigen, sondern auch die Umweltbeziehungen oder das Ansehen unseres Unternehmens erheblich beschädigen und dadurch großen Schaden verursachen. Die mit der Datenschutzgrundverordnung eingeführte Rechenschaftspflicht führt zu einer Beweislastumkehr mit der Folge, dass das Unternehmen in der Lage sein muss, die Einhaltung der Grundsätze und Vorschriften der Datenschutzgrundverordnung nachzuweisen. Dieses Datenschutzhandbuch ist ein wichtiges Instrument zur Führung dieses Nachweises und zur Erfüllung der Rechenschaftspflicht.

Das Anliegen dieses Datenschutzhandbuches ist es deshalb, im Interesse der betroffenen Personen und auch des Unternehmens den Schutz der personenbezogenen Daten nach den Vorschriften der DSGVO zu regeln und in jeder Phase der Informationsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten. Um dieses Ziel zu erreichen, müssen nicht nur die gesetzlichen Vorschriften zum Schutz der Daten eingehalten, sondern auch geeignete technische und organisatorische Maßnahmen und Verfahren eingerichtet und geregelt und deren Einhaltung und Wirksamkeit ähnlich wie nach den Methoden des Qualitätsmanagementsystems kontrolliert, dokumentiert und weiterentwickelt werden. Nicht zuletzt kommt es aber auch darauf an, dass sich alle Beschäftigten der mit dem Umgang mit personenbezogenen Daten sowie der Datenverarbeitung und der Benutzung der technischen Systeme und Kommunikationstechnologien verbundenen Risiken und Verantwortung bewusst sind und mit Daten und Systemen mit der erforderlichen Vorsicht und Sorgfalt umgehen. Bei Fragen zum Umgang mit personenbezogenen Daten ist der Vorgesetzte oder der betriebliche Datenschutzbeauftragte zu konsultieren.

* + - 1. **Zweck des Dokuments**

Das Datenschutzhandbuch folgt in der Dokumentenstruktur dem Managementhandbuch und regelt als Kopfdokument des Datenschutzmanagements mit den darin angegebenen mitgeltenden Unterlagen die rechtlichen und die zum Schutz der personenbezogenen Daten erforderlichen technischen und organisatorischen Maßnahmen. Die Einzelheiten dazu befinden sich in den mitgeltenden Unterlagen. Soweit zu einzelnen Bereichen gesonderte Dokumentationen vorhanden sind (z. B. zu bestimmten Prozessen, technischen Systemen und besonderen Verfahren), wird, sofern es zum Verständnis der Sicherungsmaßnahmen erforderlich ist, auf diese Dokumentationen verwiesen. Ebenso wird im Interesse einer besseren Pflege und Wartbarkeit dieser Richtlinien darauf verzichtet, Sicherungsmaßnahmen auf produktspezifischer Basis zu beschreiben. Insoweit werden in dieser Richtlinie die normierten Zielgrößen und Wirkungen beschrieben. Weitere Informationen befinden sich dann in den produktspezifischen Beschreibungen, Dokumentationen und mitgeltenden Unterlagen.

Das Datenschutzhandbuch beschreibt den Aufbau und die Prinzipien des Datenschutzmanagements und bezeichnet die mitgeltenden Unterlagen. Es vermittelt damit einen kompletten Überblick über den Aufbau und die Funktionsweise des Datenschutzmanagements und dient als Einstieg und Grundlage für Prüfungen und Zertifizierungen. Darüber hinaus erfüllt dieses Dokument mit den mitgeltenden Unterlagen die in der DSGVO geforderten Dokumentations- und Nachweispflichten und erfüllt die Anforderungen an die Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO.

Weil ein wirksamer Datenschutz nicht alleine durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter getragen wird, ist es ein besonderes Anliegen dieser Richtlinie, Sie für das Anliegen des Datenschutzes zu sensibilisieren und Ihnen Informationen und Regelungen an die Hand zu geben, die es ermöglichen, die mit dem Betrieb komplexer und offener Datenverarbeitungs- und Kommunikationssysteme verbundenen Risiken zu erkennen und damit umzugehen.

Dieses Datenschutzhandbuch bildet mit den enthaltenen Verweisen auf korrespondierende Dokumente und mitgeltende Unterlagen eine vollständige Beschreibung aller technischen und organisatorischen Maßnahmen und stellt damit nicht nur eine vollständige und umfassende Informationsquelle für alle Mitarbeiterinnen und Mitarbeiter dar, sondern ist auch eine Prüfgrundlage für Revisoren, Qualitätsmanager und Auditoren.

Auf der Grundlage der Bewertung der datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität der Daten und der anschließenden Einstufung in Schutz- und Vertraulichkeitsstufen konkretisieren sich die erforderlichen technischen und organisatorischen Maßnahmen. Damit besteht für Revisoren, Auditoren und auch für die Datenschutz-Aufsichtsbehörde eine fundierte und schlüssige Möglichkeit, die Vollständigkeit, Notwendigkeit und Angemessenheit der technischen und organisatorischen Maßnahmen zu beurteilen.

Bei Fragen zum Datenschutzhandbuch und zu den datenschutzrechtlichen Regelungen ist der Vorgesetzte oder der betriebliche Datenschutzbeauftragte zu konsultieren.

* + - 1. **Datenschutzgrundsätze**

Die Datenschutzgrundsätze sind in Art. 5 Abs. 1 DSGVO beschrieben und für die Verarbeitung von personenbezogenen Daten verbindlich. Die Nichtbeachtung dieser Grundsätze ist gem. Art. 83 DSGVO mit Bußgeld bedroht.

Für den Umgang mit personenbezogenen Daten werden nachfolgende Grundsätze besonders beachtet:

1. Rechtmäßigkeit

Der Grundsatz der Rechtmäßigkeit schreibt vor, dass personenbezogene Daten nur unter dem Vorbehalt einer gesetzlichen Erlaubnis oder einer Einwilligung erhoben und verarbeitet werden dürfen. Dieser Grundsatz ist in Art. 8 Abs. 2 GRCh vorgegeben und entspricht auch dem Grundsatz des Verbots mit Erlaubnisvorbehalt nach den Vorschriften der DSGVO. Bei jeder Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist deshalb darauf zu achten, dass eine Rechtsgrundlage nach den Datenschutzvorschriften vorhanden ist. Eine Rechtsgrundlage kann insbesondere ein Vertrag mit der betroffenen Person, ein berechtigtes Interesse des Unternehmens oder einer anderen Stelle unter Abwägung des Interesses und der Grundrechte und Grundfreiheiten der betroffenen Personen oder eine Einwilligung sein. Für die einzelnen Datenverarbeitungsverfahren sind die Rechtsgrundlagen in der Beschreibung zum Verzeichnis über die Verarbeitungstätigkeiten beschrieben und geprüft.

1. Verarbeitung nach Treu und Glauben

Der Grundsatz der Verarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren, und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden. Unter diesem Gesichtspunkt sind insbesondere die Rechte der Betroffenen und die Informationspflichten in verständlicher und nachvollziehbarer Form zu erfüllen. Auf die verbindlich eingerichteten Datenschutzprozesse zu den Rechten der Betroffenen und zu den Informationspflichten wird verwiesen.

1. Transparenz

Der Grundsatz der Transparenz verlangt, dass jeder Betroffene wissen soll, wer welche Daten für welche Zwecke über ihn erhebt, speichert und verarbeitet und übermittelt und wie lange die Daten gespeichert werden, und dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Natürliche Personen sind über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. Hier sind die im Einzelnen geregelten Informationspflichten zu beachten (vgl. dazu den Datenschutzprozess „Modalitäten für die Ausübung der Rechte, Verfahrensvorschriften“).

1. Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.Die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Eine Verarbeitung oder Nutzung von personenbezogenen Daten für andere als den Betroffenen im Zusammenhang mit der Datenerhebung kommunizierten Zwecke ist nur unter den gesetzlich festgelegten Bedingungen (Art. 6 Abs. 4 DSGVO) und ansonsten nur mit Einwilligung der Betroffenen zulässig. Sollen erhobene Daten auch für einen anderen als den der Erhebung zugrunde liegenden Zweck verwendet werden, z. B. zu Zwecken der Werbung oder des Profilings oder für Datenübermittlungen, ist vorher der Datenschutzbeauftragte zu konsultieren.

1. Datenminimierung

Art und Umfang der Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dies schließt eine Begrenzung der Speicherfrist auf das erforderliche Mindestmaß ein. Hier ist darauf zu achten, dass nur diejenigen Daten von den Betroffenen erhoben werden, die für den jeweiligen Verarbeitungszweck auch wirklich erforderlich sind. Darüber hinausgehende Erhebungen und Verarbeitungen sind unzulässig. Zweifelsfragen zur Erforderlichkeit der Daten und zur Zulässigkeit der Datenverarbeitung sind mit dem Vorgesetzten oder dem Datenschutzbeauftragten abzuklären.

1. Richtigkeit

Die personenbezogenen Daten müssen im Hinblick auf die Zwecke ihrer Verarbeitung sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Verarbeitung unrichtiger Daten ist zu vermeiden. Unrichtige Daten sind unverzüglich zu berichtigen.

1. Nachvollziehbarkeit, Revisionsfähigkeit

Die Verarbeitung und die Veränderung von personenbezogenen Daten müssen nachvollziehbar und, soweit erforderlich, in geeigneter Weise dokumentiert und überprüfbar sein. Einzelheiten, insbesondere zur Nachvollziehbarkeit und zu Protokollierungen, sind mit dem Datenschutzbeauftragten abzustimmen und zu regeln.

1. Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie erhoben worden sind, erforderlich ist. Um sicherzustellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden, sind Fristen für ihre Löschung oder regelmäßige Überprüfung vorzusehen und die Daten regelmäßig zu löschen bzw. zu vernichten. Die Aufbewahrungsfristen sind von den fachverantwortlichen Stellen festzulegen und die Löschung bzw. Vernichtung der Daten ist von diesen Stellen zu veranlassen, zu überwachen und, soweit erforderlich, zu dokumentieren. Die Verfahren für eine sichere Löschung von personenbezogenen Daten und die Vernichtung/Entsorgung von Geräten und Datenträgern sind mit dem betrieblichen Datenschutzbeauftragten abzustimmen.

1. Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit verlangt einen angemessenen Schutz und eine angemessene Sicherheit der personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Bei der Verarbeitung der personenbezogenen Daten ist durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten.

1. Rechenschaftspflicht

Der Grundsatz der Rechenschaftspflicht verlangt, dass die Einhaltung der o. g. Datenschutzgrundsätze nachgewiesen werden kann. Zur Erfüllung dieser Rechenschaftspflicht ist ein in sich stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet. Auf der Grundlage der dazu geführten Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich. Die in diesem Datenschutzhandbuch zu diesem Zweck festgelegten Dokumentationen und Nachweise sind aktuell und vollständig zu führen.

Für die Beachtung dieser Grundsätze und für die Gestaltung und Einhaltung der hierfür erforderlichen Regelungen ist die für den jeweiligen Fachprozess zuständige Stelle verantwortlich. Bei Zweifelsfragen zur Interpretation der Grundsätze und deren Anwendung ist der betriebliche Datenschutzbeauftragte zu konsultieren.

* + - 1. **Datenschutzorganisation**

1. Bestellung eines betrieblichen Datenschutzbeauftragten

Das Gesetz zur Anpassung des Datenschutzrechts an die Vorschriften der DSGVO (DSAnpUG-EU) schreibt für unser Unternehmen die Bestellung eines Datenschutzbeauftragten vor. Der Datenschutzbeauftragte kann eine externe oder eine unternehmensinterne Person sein. Es ist ein interner <*alternativ externer*> Datenschutzbeauftragter bestellt. Der Datenschutzbeauftragte ist gem. Art. 37 Abs. 7 DSGVO der Aufsichtsbehörde für den Datenschutz gemeldet.

Für den Datenschutzbeauftragten gelten folgende Regelungen:

* + 1. Organisatorische Einrichtung im Unternehmen

Der Datenschutzbeauftragte ist unmittelbar der Geschäftsleitung (*ggf. nähere Bezeichnung der Stelle*) unterstellt und berichtet an (*Bezeichnung der Stelle*). Näheres zur organisatorischen Einrichtung ist in der Stellenbeschreibung <*alternativ: im Bestellungsvertrag*> beschrieben. Zu seiner Unterstützung sind im erforderlichen Umfang Datenschutzkoordinatoren bestellt.

* + 1. Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten sind folgende Aufgaben übertragen:

* 1. Unterrichtung und Beratung der Geschäftsleitung und der Beschäftigten in allen Datenschutzfragen
  2. Überwachung der Einhaltung der Datenschutzvorschriften
  3. Sensibilisierung und Schulung/Unterweisung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
  4. Durchführung von Datenschutzprüfungen nach eigenem Ermessen und im Auftrag der Geschäftsleitung
  5. Datenschutzrechtliche Freigabe von automatisierten Datenverarbeitungsverfahren zur Verarbeitung von personenbezogenen Daten und von datenschutzrelevanten Änderungen zur Anwendung. Die Freigabe erfolgt i. d. R. mit der Beschreibung der Verarbeitungsverfahren im Verzeichnis der Verarbeitungstätigkeiten und den damit verbundenen datenschutzrechtlichen Prüfungen.
  6. Beratung und Unterstützung bei der Zusammenarbeit mit der Aufsichtsbehörde (*Hinweis:* *Das nähere Verfahren, insbesondere Vertretungs- und Zeichnungsbefugnisse, ist hier zu regeln.*)
     1. Informations- und Informationszugangsrechte des Datenschutzbeauftragten

Der Datenschutzbeauftragte besitzt im Zusammenhang mit seiner Tätigkeit ein uneingeschränktes Informationsrecht zu allen Fragen des Umgangs mit personenbezogenen Daten und ein uneingeschränktes Zugangsrecht zu allen damit zusammenhängenden Unterlagen, Informationen und Dokumenten. Die Unterlagen sind dem Datenschutzbeauftragten auf Verlangen vollständig und unverzüglich in geeigneter Weise zur Verfügung zu stellen.

* + 1. Datenschutzberichte

Der Datenschutzbeauftragte berichtet regelmäßig (mindestens einmal jährlich) der

o. g. Stelle über seine Tätigkeit und über seine Feststellungen (Jahresbericht). Bei besonderen Vorkommnissen berichtet er unverzüglich und unterrichtet die beteiligten Stellen zur Einleitung der erforderlichen Maßnahmen.

In seinem Jahresbericht beurteilt der Datenschutzbeauftragte nach dem vorgegebenen Dokumentations- und Bewertungssystem den Stand des Datenschutzes und in Abstimmung mit dem IT-Sicherheitsverantwortlichen auch den Stand der technischen und organisatorischen Maßnahmen zum Datenschutz.

Der Datenschutzbeauftragte berät in allen Fragen des Datenschutzes und soll, soweit möglich, auch bereits präventiv tätig sein. Aus diesem Grund ist er von den fachbereichs- bzw. projektverantwortlichen Stellen insbesondere bei den folgenden Vorhaben frühzeitig einzubeziehen:

* Neuentwicklung oder Änderung von IT-Systemen
* Einführung von Systemen zur Personal- oder Kundendatenverarbeitung
* Gestaltung der Telekommunikations-, Internet-, Intranet- oder E-Mail-Nutzung
* Abschluss von Betriebsvereinbarungen mit Bezug zum Umgang mit Mitarbeiterdaten
* Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag (Outsourcing)
* Übermittlung von personenbezogenen Daten an Stellen außerhalb des Unternehmens
* Gestaltung von Datenerhebungen für automatisierte Verfahren

Jeder von der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch die <*Name der* *Firma*> Betroffene kann sich an den Beauftragten für den Datenschutz wenden. Ebenso kann sich jeder Mitarbeiter in allen Fragen des Datenschutzes an ihn wenden. Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen verpflichtet, soweit er nicht durch den Betroffenen davon entbunden ist.

* + - 1. Konzernübergreifende Datenschutzorganisation, Konzerndatenschutzbeauftragter

Für konzernübergreifende Datenschutzfragen ist bei <*Stelle, Unternehmen*> ein Konzerndatenschutzbeauftragter/Datenschutzkoordinator bestellt.

Aufgaben des Konzerndatenschutzbeauftragten

<*Beschreibung der Aufgaben*>

Zusammenarbeit des betrieblichen Datenschutzbeauftragten mit dem Konzerndatenschutzbeauftragten

<*Beschreibung bzw. Regelungen für die Zusammenarbeit*>

* + - 1. Datenschutz und Betriebsrat

Der betriebliche Datenschutzbeauftragte hat beim Betriebsrat keine Prüfrechte und der Datenschutzbeauftragte unterliegt keinen Weisungen des Betriebsrats. Der Betriebsrat kann aber den Datenschutzbeauftragten in Datenschutzfragen konsultieren. Unbeschadet der Unabhängigkeit des Betriebsrats hat der Betriebsrat die rechtlichen und sicherheitsrelevanten Anforderungen des Datenschutzes und die hierzu ergangenen betrieblichen Regelungen zu beachten. Abweichungen von den betrieblichen Regelungen aufgrund der besonderen Stellung des Betriebsrats sind vom Betriebsrat mit den beteiligten Stellen abzustimmen.

**Mitgeltende Unterlagen:**

* Bestellung des betrieblichen Datenschutzbeauftragten <*alternativ Vertrag über die Bestellung eines externen Datenschutzbeauftragten*>
* Ggf. Bestellung von Datenschutzkoordinatoren
* Stellenbeschreibung des Datenschutzbeauftragten
* Mitarbeiterinformation über die Bestellung des Datenschutzbeauftragten
* Kontaktdaten des betrieblichen Datenschutzbeauftragten
* Angaben zum Konzerndatenschutzbeauftragten

1. **Datenschutzmanagement**
   1. Integration des Datenschutzmanagements in das Unternehmensmanagement

Die Erfüllung der operativen Aufgaben des Datenschutzes bzw. die Ausführung der vorgeschriebenen Maßnahmen und Regelungen ist den für die einzelnen Fachbereiche bzw. für die Geschäftsprozesse verantwortlichen Fachbereichsleitern bzw. Geschäftsprozessverantwortlichen übertragen. Die für die einzelnen Geschäftsprozesse bzw. Fachbereiche relevanten Datenschutzvorgaben sind in den Datenschutzprozessen und in den Verfahrensbeschreibungen zur Übersicht über die Verarbeitungstätigkeiten verbindlich festgelegt. Die Vollständigkeit und Aktualität der Datenschutzprozesse und Verfahrensbeschreibungen wird vom betrieblichen Datenschutzbeauftragten regelmäßig überprüft.

* 1. Qualitätsmanagement
     1. Verankerung des Datenschutzes in den QM-Dokumenten

Die datenschutzrechtlichen Vorgaben zu Unternehmenszielen und Strategien werden in den zutreffenden QM-Dokumenten beschrieben und ausgestaltet. Der QM-Verantwortliche und der Datenschutzbeauftragte wirken gemeinsam auf die Entwicklung geeigneter Datenschutzziele und -strategien hin. Der Datenschutzbeauftragte hat für die Entwicklung der Datenschutzziele und Strategien eine besondere Beratungsaufgabe. Für die förmliche Ausgestaltung in der QM-Dokumentation ist der QM-Beauftragte verantwortlich.

* + 1. Integration des Datenschutzes in den PDCA-Zyklus/Kontinuierlichen Verbesserungsprozess

Zur laufenden Aktualisierung und Fortentwicklung des Datenschutzes und zur Anpassung an sich verändernde Verhältnisse im Unternehmen ist der Datenschutz in den PDCA-Zyklus bzw. den Kontinuierlichen Verbesserungsprozess nach den eingerichteten Regeln des Qualitätsmanagements integriert. Der Datenschutzbeauftragte beobachtet die Rechtsentwicklung im Datenschutz und wendet für seinen Bereich in Abstimmung mit dem QM-Verantwortlichen die Prinzipien des PDCA-Zyklus an.

* + 1. Integration des Datenschutzes in das Auditwesen

Der Qualitätsmanagement- und ggf. der Informationssicherheitsverantwortliche stimmen den internen und den externen Auditplan sowie die Beteiligung des Datenschutzbeauftragten an den Auditierungen mit dem Datenschutzbeauftragten ab. Die sich aus der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO ergebenden Anforderungen hinsichtlich der Auditierungen und der Nachweisführung sind zu berücksichtigen.

<*Alternativ*>

Der Datenschutzbeauftragte kann einen jährlichen Prüfplan über die durchzuführenden Datenschutzprüfungen erstellen. Die Prüfungen sind so zu gestalten, dass alle datenschutzrelevanten Bereiche, Prozesse und Datenverarbeitungsverfahren in einem angemessenen Rhythmus dahingehend überprüft und bewertet werden, ob die Anforderungen der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO erfüllt werden.

**Mitgeltende Unterlagen:**

* Übersicht über die eingerichteten Datenschutzprozesse
* Ggf. Prüfplan des betrieblichen Datenschutzbeauftragten
* Auditplan

Soweit kein QM-Management eingerichtet ist, sind hier zu nennen:

* Datenschutzziele und Strategien
* Datenschutzprüfplan
* Bewertung des Standes des Datenschutzes

1. **Datensicherheitsmanagement**
   1. Integration des Datensicherheitsmanagements in das Informations- und

IT-Sicherheitsmanagement

* + 1. Bestehende Normen und Zertifikate

Es bestehen zu folgenden Bereichen/Prozessen Zertifizierungen auf der Grundlage <*Normengrundlage angeben*>.

* + 1. Berücksichtigung des Datenschutzes in den Zielen und Maßnahmen der Norm

Die Forderungen des Datenschutzes sind in den Zielen und Maßnahmen der <*Norm angeben*> beschrieben. Besondere Anforderungen des Datenschutzes und die speziellen technischen und organisatorischen Maßnahmen dazu sind in den einzelnen Nachweisdokumenten beschrieben.

* + 1. Definition der Datenschutzanforderungen der beteiligten Parteien

Die beteiligten Parteien (Stakeholder) sind zu identifizieren und deren Datenschutzanforderungen bzw. Erwartungen an den Datenschutz zu beschreiben. Für die Identifizierung der Stakeholder und deren Datenschutzerwartungen ist der jeweilige Fachbereich zuständig. Die Beschreibung und Dokumentation erfolgt in Abstimmung mit dem QM-Verantwortlichen und dem betrieblichen Datenschutzbeauftragten. <*Alternativ: Zu konzernübergreifenden Gesichtspunkten ist der Konzerndatenschutzbeauftragte zuzuziehen.*>

* + 1. Technische und organisatorische Maßnahmen zum Informations- und Datenschutz

Die beschriebenen Normen und technischen und organisatorischen Maßnahmen gelten auch für die personenbezogenen Daten. Soweit sich für die personenbezogenen Daten zusätzliche Anforderungen ergeben, sind diese dort ebenfalls zu berücksichtigen.

**Mitgeltende Unterlagen:**

* Zertifikate und Normen

1. **Schutzziele und Schutzgrade der Daten, Vertraulichkeitsrichtlinie**

**Schutzeinstufung**

Die einzelnen Datenverarbeitungsverfahren werden nach dem Grad ihrer datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität beurteilt und einer Schutzstufe zugeordnet. Die Schutzeinstufungen sind eine mitgeltende Unterlage zur Beschreibung der einzelnen Verarbeitungsverfahren im Verzeichnis der Verarbeitungstätigkeiten. Die datenschutzrechtliche Sensibilität der personenbezogenen Daten beurteilt sich an der Frage, inwieweit der Betroffene bei einer Datenschutzverletzung in seinen Persönlichkeitsrechten oder seinem persönlichen oder wirtschaftlichen Ansehen verletzt oder eingeschränkt ist bzw. verletzt oder eingeschränkt werden kann.

Die Schutzstufe des gesamten Datenverarbeitungsverfahrens richtet sich nach den Schutzanforderungen der sensibelsten Datenkategorien des zugehörigen Datenbestands. Es bestehen aber für die personenbezogenen und sonstigen vertraulichen Daten noch weitere Schutzziele, und zwar die Gewährleistung der Verfügbarkeit, der Schutz der Integrität, der Authentizität und der Revisionsfähigkeit. Diese Schutz­ziele können je nach Schutzbedarf der Daten unterschiedlich hoch ausgeprägt sein und werden bei Bedarf nach der in der nachstehenden Tabelle dargestellten Skalierung festgelegt.

Die Festlegung der Schutzziele und deren Skalierung trifft die über die Informationen und Daten verfügungsberechtigte Stelle.

Der Schutzgrad orientiert sich an dem Ausmaß der Verletzung des Persönlichkeitsrechts der Betroffenen und an der Höhe des Schadens, der sowohl dem Betroffenen als auch dem Unternehmen entstehen kann. Unter Datenschutzgesichtspunkten ist insbesondere auch dem erhöhten Schutz der besonderen Datenarten im Sinne von Art. 9 DSGVO Rechnung zu tragen.

Kriterien für die Festlegung der Schutzziele sind weitere gesetzliche Anforderungen an die Daten, die sich aus ihrer jeweiligen Rechtsnatur ergeben, z. B. nach steuer- und handelsrechtlichen Vorschriften, den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) oder der ordnungsgemäßen Datenverarbeitung (GoDV) u. a., und Anforderungen unter dem Gesichtspunkt der Beweiskraft und Gerichtsverwertbarkeit der Informationen und Daten.

In Abhängigkeit von den Schutzzielen sind bei Bedarf von den fachverantwortlichen Stellen nach den Vorgaben in der Tabelle die im Einzelnen erforderlichen technischen und organisatorischen Maßnahmen abzuleiten und festzulegen. Dazu gehören:

* Die Festlegung der Verfügbarkeit, d. h. der maximal tolerierbaren Ausfallzeit der Daten
* Die Festlegung von Rechten an den Daten, insbesondere der Rechteprofile der Benutzer der Datenverarbeitungsverfahren, von Protokollierungen von Zugriffen und Veränderungen sowie ggf. von Signaturen zum Nachweis der Integrität der Daten
* Die Festlegung von Maßnahmen zum Nachweis der Authentizität der Daten, z. B. Protokollierung der Einstellung und Veränderung der Daten in Datenverarbeitungsverfahren bzw. elektronische Signatur
* Die Festlegung von Dokumentationen, Freigaben und Protokollierungen zum Nachweis der Revisionsfähigkeit der Datenverarbeitungsverfahren und der Daten

Der Umgang mit besonders vertraulichen Daten und Informationen ist in einer Vertraulichkeitsrichtlinie gesondert geregelt. In dieser Richtlinie sind die besonders vertraulichen Daten und Informationen ihrer Art nach definiert und die Verantwortlichkeiten sowie der Umgang mit diesen Daten gesondert geregelt.

**Mitgeltende Unterlagen:**

* Verzeichnis über Verarbeitungstätigkeiten
* Vertraulichkeitsrichtlinie

1. **Datenschutzdokumente**

Die Datenschutzdokumentation enthält folgende Dokumente:

* 1. Übersicht über die eingerichteten Datenschutzprozesse

Die Übersicht enthält alle gültigen und verbindlich eingerichteten Datenschutzprozesse und für jeden Prozess ein grafisches Modell mit einer Kurzbeschreibung. Für jeden Datenschutzprozess sind die zuständige Stelle, sonstige zu beteiligende sowie zu informierende Stellen, das Prüfintervall für die Prüfung durch den betrieblichen Datenschutzbeauftragten und die mitgeltenden Unterlagen festzulegen.

* 1. Verzeichnis über die Verarbeitungstätigkeiten

Gemäß Art. 30 Abs. 1 DSGVO wird ein Verzeichnis über die Verarbeitungstätigkeiten geführt. Das Verzeichnis wird von <*Bezeichnung der Stelle*> geführt. Das Verzeichnis besteht aus den folgenden Dokumenten:

* + 1. Übersicht über die Datenverarbeitungsverfahren und gemeinsame Angaben

Um überflüssige Wiederholungen und Redundanzen zu vermeiden, werden die gemeinsamen Angaben zum Verzeichnis über die Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 lit. a DSGVO in einem Formular „Gemeinsame Angaben zum Verzeichnis über die Verarbeitungstätigkeiten“ vorangestellt. Diese gemeinsamen Angaben enthalten auch eine Auflistung der einzelnen Datenverarbeitungsverfahren, die in den zugehörigen Beschreibungen der einzelnen Verfahren ausführlich beschrieben sind.

* + 1. Beschreibung der einzelnen Verfahren

Die Beschreibung der einzelnen Verfahren enthält die Angaben lt. Art. 30

Abs. 1 lit. b bis f DSGVO. Die Beschreibung der Verfahren für Verantwortliche gem. Art. 30 Abs. 1 DSGVO enthält über die Pflichtangaben des Art. 30 Abs. 1 DSGVO hinaus alle zur Prüfung der Rechtmäßigkeit des Verfahrens und der Verarbeitung erforderlichen Angaben und unter Angabe der Rechtsgrundlage auch eine Prüfung der Zulässigkeit der einzelnen Verarbeitungstätigkeiten und der Erfüllung der datenschutzrechtlichen Voraussetzungen. Der Datenschutzbeauftragte bestätigt auf jeder einzelnen Verfahrensbeschreibung die datenschutzrechtliche Ordnungsmäßigkeit bzw. Konformität des Verfahrens und vermerkt das Datum der letzten Prüfung des Verfahrens. Stellt der Datenschutzbeauftragte bei der Prüfung eines Datenverarbeitungsverfahrens Abweichungen fest, vermerkt er diese bei der Verfahrensbeschreibung und berichtet der Geschäftsleitung. Der Datenschutzbeauftragte überwacht die Erledigung der Abweichungen.

* + 1. Beschreibung der Auftragsdatenverarbeitungen

Die Beschreibung der Auftragsdatenverarbeitungen gem. Art. 30 Abs. 2 DSGVO enthält eine Übersicht über alle Datenverarbeitungsverfahren, die im Auftrag für andere Stellen durchgeführt werden. Für die Führung dieses Verzeichnisses ist <*Bezeichnung der Stelle*> zuständig. Die für die Verfahren zuständigen Stellen melden neue Verfahren rechtzeitig der <*Bezeichnung der Stelle*> und unterrichten den betrieblichen Datenschutzbeauftragten.

* + 1. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Diese Beschreibung enthält die übergreifenden und für alle Verarbeitungsverfahren gültigen allgemeinen technischen und organisatorischen Maßnahmen. Bestehende Verfahrensanweisungen und Regelungen zu den technischen und organisatorischen Maßnahmen werden als mitgeltende Unterlagen geführt. Soweit für einzelne Verfahren davon abweichende verfahrensindividuelle Maßnahmen bestehen, sind diese in den Verfahrensbeschreibungen zu den einzelnen Verfahren enthalten.

* 1. Risikobewertung und Verfahren zur Klassifizierung der personenbezogenen Daten nach Risikostufen und Schutzbedarfsfeststellung

Das Risiko wird aus der Sicht der Betroffenen beurteilt und in folgende drei Risikostufen (Schutzklassen) eingeteilt:

* + - Kein rechtserhebliches (geringes) Risiko
    - Mittleres, das allgemein vorhandene Risiko (Grundrisiko) übersteigende Risiko
    - Hohes Risiko

Die Risiken und Risikogruppen sowie deren Eintrittswahrscheinlichkeit und Schwere sowie die daraus abzuleitende Schutzklasse der Daten sind zu ermitteln und zu dokumentieren. Das Ergebnis ist in der Verfahrensbeschreibung des Verzeichnisses über die Verarbeitungstätigkeiten zu den einzelnen Datenverarbeitungsverfahren anzugeben. Für die Risikobewertung ist die für das jeweilige Verarbeitungsverfahren zuständige Stelle verantwortlich. Bei der Erstellung der Risikobewertung und bei Änderungen der Bewertung ist der betriebliche Datenschutzbeauftragte zuzuziehen.

* 1. Checklisten und Dokumentationen über die Erhebungen des Datenschutzbeauftragten zum Datenschutz und zur Datensicherheit und Bewertung des Standes des Datenschutzes und der technischen und organisatorischen Maßnahmen

Zum Nachweis der Einhaltung der datenschutzrechtlichen Vorschriften ist ein Dokumentations- und Bewertungsverfahren eingerichtet. Im Rahmen dieses Verfahrens werden die einzelnen datenschutzrechtlichen Sachverhalte anhand von vorgegebenen Checklisten erhoben und nach ihrem Erfüllungsgrad bewertet. Diese Checklisten sind ein Teil der verbindlichen Datenschutzdokumentation. Sie vermitteln einerseits einen vollständigen Überblick über alle datenschutzrechtlich relevanten Sachverhalte und deren Überprüfung und zeigen den Grad der Erfüllung der einzelnen datenschutzrechtlichen Voraussetzungen sowie eventuell noch offene Handlungsbedarfe. Anhand der Checklisten und einer Bewertungstabelle wird eine Bewertung des Erfüllungsgrades erstellt und damit der Nachweis zur Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO geführt.

* 1. Verantwortlichkeit für die Führung der Datenschutzdokumentation

Für die laufende Ergänzung und Aktualisierung der Datenschutzdokumentation, der Checklisten, des Dokumentations- und Bewertungssystems nach den ihm vorgelegten Meldungen und Informationen und für die regelmäßige Bewertung des Standes des Datenschutzes ist der betriebliche Datenschutzbeauftragte verantwortlich.

**Mitgeltende Unterlagen:**

* Risiko- und Schutzbedarfsermittlung
* Übersicht über die eingerichteten Datenschutzprozesse
* Verzeichnis über die Verarbeitungstätigkeiten
* Beschreibung der technischen und organisatorischen Maßnahmen
* Checklisten lt. Übersicht des Datenschutzbeauftragten
* Bewertungstabellen

1. **Datenschutzprozesse und Verfahren**

Der Datenschutzbeauftragte überwacht die Führung einer verbindlichen Übersicht über die eingerichteten Datenschutzprozesse. Er legt mit den für die Fachprozesse bzw. Fachbereiche verantwortlichen Stellen die zugehörigen verbindlichen Checklisten fest. Die zugehörigen Verfahrensanweisungen werden vom zuständigen Fachbereichsverantwortlichen bzw. von den für den jeweiligen Fachprozess verantwortlichen Stellen verwaltet.

Der Bestand dieser Datenschutzprozesse wird vom Datenschutzbeauftragten regelmäßig geprüft und ggf. ergänzt. Die Datenschutzprozesse werden anhand der Checklisten in den festgelegten Prüfintervallen geprüft und bewertet.

**Mitgeltende Unterlagen:**

* Übersicht über die eingerichteten Datenschutzprozesse
* Checklisten lt. Übersicht des Datenschutzbeauftragten

1. **Rechte der Betroffenen**

Vorgänge über die Wahrnehmung von Rechten der Betroffenen (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. des Rechts auf Datenübertragbarkeit.) werden von <*Bezeichnung der Stelle*> bearbeitet und dokumentiert und sind dieser unverzüglich zuzuleiten. Die <*Bezeichnung der Stelle*> regelt das weitere Verfahren nach den dazu bestehenden Datenschutzprozessen und veranlasst die umgehende Einschaltung des Datenschutzbeauftragten. Die Bearbeitung von Anträgen der Betroffenen zur Wahrnehmung ihrer Rechte ist eng mit dem Datenschutzbeauftragten abzustimmen.

Beschwerden der Betroffenen in Datenschutzangelegenheiten werden ebenfalls von <*Bezeichnung der Stelle*> nach den Vorgaben des Beschwerdemanagements bearbeitet und sind dem Datenschutzbeauftragten zu melden.

**Mitgeltende Unterlagen:**

* Datenschutzprozesse über die Rechte der Betroffenen
* Dokumentation der bearbeiteten Vorgänge zu den Rechten der Betroffenen

1. **Information der Betroffenen bei der Datenerhebung**

Bei jeder Datenerhebung von den betroffenen Personen sind die Betroffenen in geeigneter Weise (z. B. durch einen schriftlichen Hinweis) über die in Art. 13 DSGVO genannten Sachverhalte zu informieren. Die Modalitäten des Art. 12 DSGVO sind dabei zu beachten.

Wenn die Daten nicht von der betroffenen Person erhoben worden sind, sind die Betroffenen fristgerecht (siehe Art. 14 Abs. 3 DSGVO) zu unterrichten. Die fachverantwortlichen Stellen sind für die Durchführung der vorgeschriebenen Informationen verantwortlich. Inhalt und Verfahren zur Information der betroffenen Personen sind mit dem betrieblichen Datenschutzbeauftragten abzustimmen.

Jeder Fachbereichsverantwortliche und der IT-Verantwortliche <*ggf. konkretere Bezeichnung der Stellen*> ist jeweils für seinen Bereich auch dafür verantwortlich, dass in der Datenschutzerklärung zum Internetauftritt des Unternehmens die erforderlichen Informationen zum Datenschutz enthalten sind.

Die Art und Weise der Unterrichtung sowie deren Form und Inhalt sowie die Datenschutz­er­­klärung zum Internetauftritt sind mit dem Datenschutzbeauftragten abzustimmen.

**Mitgeltende Unterlagen:**

* Datenschutzprozess „Informationspflicht bei einer Datenerhebung vom Betroffenen“
* Datenschutzprozess „Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden“
* Datenschutzinformation der Betroffenen

1. **Meldung von Datenschutzverletzungen**

Bei einer möglichen Verletzung des Schutzes von personenbezogenen Daten, insbesondere bei einem Verlust der Vertraulichkeit durch eine unbefugte Offenbarung oder Datenübermittlung, unbefugte Zugriffe oder Verarbeitungen oder durch Verlust, Zerstörung oder Verfälschung der Daten, ist sofort der jeweilige Vorgesetzte zu informieren. Dieser leitet umgehend die erforderlichen Sofortmaßnahmen zur Behebung der Ursachen der Datenschutzverletzung ein und benachrichtigt die beteiligten Stellen, die Geschäftsleitung und den Datenschutzbeauftragten. Für die Vorgehensweise bei der Bearbeitung von Datenschutzverletzungen ist der Prozess „Melde- und Benachrichtigungspflicht“ und die Dokumentation zur Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DSGVO verbindlich.

Die Meldung an die Aufsichtsbehörde für den Datenschutz und die Information der Betroffenen erteilt die Geschäftsleitung. Für die Meldung an die Aufsichtsbehörde ist eine Frist von 72 Stunden einzuhalten. Die <*Bezeichnung der Stelle*> führt eine Übersicht über die Vorfälle.

Die Sicherheitsvorfälle sind nach den Vorgaben der „IT-Sicherheitsrichtlinie – Einsatz und Nutzung der IT-Systeme“ aufzuarbeiten.

Vorfälle bei Auftragsdatenverarbeitungen

Bei einer möglichen Verletzung des Schutzes von personenbezogenen Daten, insbesondere bei einem Verlust der Vertraulichkeit durch eine unbefugte Offenbarung oder Datenübermittlung, unbefugte Zugriffe oder Verarbeitungen oder durch Verlust, Zerstörung oder Verfälschung der Daten oder eine sonstige Störung der Auftragsdatenverarbeitung, ist sofort der jeweilige Vorgesetzte zu informieren. Dieser leitet umgehend die erforderlichen Sofortmaßnahmen zur Behebung der Ursachen der Störung bzw. Datenschutzverletzung ein und benachrichtigt die beteiligten Stellen, die Geschäftsleitung und ggf. den Datenschutzbeauftragten.

Die Geschäftsleitung entscheidet über die weitere Vorgehensweise auf der Grundlage des bestehenden Vertrags über die Auftragsdatenverarbeitung und unterrichtet ggf. den Auftraggeber. Die <*Bezeichnung der Stelle*> führt eine Übersicht über die Vorfälle.

**Mitgeltende Unterlagen:**

* Datenschutzprozess „Melde- und Benachrichtigungspflicht“
* Formular zur Dokumentation zur Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DSGVO
* IT-Sicherheitsrichtlinie – Einsatz und Nutzung der IT-Systeme
* Dokumentation der Datenschutzvorfälle

1. **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

* 1. Beschaffung von Software

Bei der Beschaffung von Software zur Verarbeitung von personenbezogenen Daten ist auf die Erfüllung der Anforderungen hinsichtlich einer datenschutzfreundlichen Technikgestaltung zu achten. Kriterien für eine datenschutzfreundliche Technikgestaltung sind insbesondere eine Minimierung der Verarbeitung von personenbezogenen Daten und deren frühzeitige Pseudonymisierung, eine Rechtegestaltung nach dem Minimalprinzip sowie Funktionen zur Unterstützung der Wahrnehmung der Rechte der Betroffenen, insbesondere des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. des Rechts auf Datenübertragbarkeit. Die ausreichende Erfüllung dieser Anforderungen ist ein Auswahlkriterium.

* 1. Softwareentwicklung

Bei der Softwareentwicklung sind ebenfalls die unter a. bezeichneten Anforderungen zu beachten und zu erfüllen.

* 1. Implementation von Datenverarbeitungsverfahren

Bei der Implementierung von Verfahren zur Verarbeitung von personenbezogenen Daten ist auf Beschränkung des Funktionsumfangs, eine Minimierung von personenbezogenen Daten, auf eine Rechtebeschränkung auf den nötigen Umfang und die Nutzung von Sicherheitsfunktionen zu achten.

Einzelheiten sind ggf. mit dem Datenschutzbeauftragten abzustimmen. Die Maßnahmen, Vorkehrungen und Funktionen zur datenschutzfreundlichen Technikgestaltung und zum datenschutzfreundlichen Design sind zu dokumentieren.

**Mitgeltende Unterlagen:**

* Dokumentationen über die eingerichteten Funktionen zum Datenschutz durch Technikgestaltung

1. **Datenschutzfolgenabschätzung und vorherige Konsultation der Aufsichtsbehörde gem. Art. 35 u. 36 DSGVO**

Durchführung der Datenschutzfolgenabschätzung

Die Datenschutzfolgenabschätzung ist von dem für die Verarbeitung der personenbezogenen Daten verantwortlichen Fachbereich nach den Vorgaben des Datenschutzprozesses „Datenschutzfolgenabschätzung“ durchzuführen. Der betriebliche Datenschutzbeauftragte ist beratend zuzuziehen.

In einer Risikobeurteilung ist zunächst zu ermitteln, ob die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Ist dies nicht der Fall, ist keine Datenschutzfolgenabschätzung durchzuführen und das Ergebnis der Beurteilung zu dokumentieren. Ergibt die Beurteilung, dass die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt, ist eine Datenschutzfolgenabschätzung nach den Regelungen des Datenschutzprozesses „Datenschutzfolgenabschätzung“ durchzuführen. Das Ergebnis der Risikobeurteilung und ggf. einer Datenschutzfolgenabschätzung ist in der Beschreibung des Verfahrens zur Übersicht über die Verarbeitungstätigkeiten zu vermerken.

Zur Beherrschung der Risiken für die Rechte und Freiheiten der betroffenen Personen sind geeignete technische und organisatorische Maßnahmen zu entwickeln und zu dokumentieren. Verbleibt trotzdem für die Rechte und Freiheiten der betroffenen Personen ein hohes Restrisiko, ist die Geschäftsführung zu unterrichten. Die Geschäftsführung entscheidet über die Einstellung oder Weiterentwicklung des Verfahrens und veranlasst im Fall einer Weiterentwicklung die vorherige Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO.

**Mitgeltende Unterlagen:**

* Prozess und Checkliste zur Datenschutzfolgenabschätzung
* Dokumentation der Risikobeurteilung
* Dokumentation der Datenschutzfolgenabschätzung
* Verfahrensbeschreibung zur Übersicht über die Verarbeitungstätigkeiten

1. **Vertraulichkeit und Geheimhaltungspflichten**

Die personenbezogenen Daten unterliegen der Vertraulichkeit gem. Art. 5 Abs. 1 DSGVO. Soweit personenbezogene Daten sonstigen Geheimnissen bzw. Geheimhaltungsvorschriften unterliegen, sind diese Geheimhaltungspflichten in der Übersicht über die Verarbeitungstätigkeiten bei den einzelnen Verarbeitungsverfahren zu dokumentieren, die Beschäftigten über diese Geheimhaltungs- bzw. Schweigepflichten nachweisbar zu unterrichten und auf die Einhaltung dieser Geheimhaltungsvorschriften zu verpflichten. Geheimnisse dieser Art können insbesondere das Telekommunikationsgeheimnis, Berufsgeheimnisse, vertragliche Geheimhaltungspflichten (z. B. aus Verträgen mit Kunden) oder Betriebsgeheimnisse sein.

**Mitgeltende Unterlagen:**

* Verpflichtung auf die Wahrung der Vertraulichkeit
* Ggf. weitere sonstige Geheimhaltungsvorschriften und Verpflichtungen
* Verfahrensbeschreibung zur Übersicht über die Verarbeitungstätigkeiten

1. **Datenverarbeitung im Auftrag**
   1. Auswahl und Kontrolle der Auftragnehmer

Bei der Auswahl der Auftragnehmer für eine Datenverarbeitung im Auftrag ist darauf zu achten, ob der Auftragnehmer durch technische und organisatorische Maßnahmen hinreichende Garantien für den Schutz der Rechte der betroffenen Personen bietet. Die eingerichteten technischen und organisatorischen Maßnahmen sind in Abstimmung mit dem Datenschutzbeauftragten in geeigneter Weise zu überprüfen. Die Überprüfung ist zu dokumentieren.

* 1. Verträge über eine Datenverarbeitung im Auftrag

Über die Beauftragungen sind Verträge nach den Vorgaben des Art. 28 DSGVO abzuschließen bzw. entsprechende Ergänzungen vorzunehmen. Zum Vertragsabschluss und ggf. zu eventuellen Vertragsergänzungen ist der Datenschutzbeauftragte hinzuzuziehen. Bei einer Vergabe von Unteraufträgen ist darauf zu achten, dass die vertraglichen Verpflichtungen, denen <*Bezeichnung des Unternehmens*> gegenüber dem Auftraggeber unterliegt, in gleicher Weise an den Unterauftragnehmer weitergegeben werden.

* 1. Übersicht über Beauftragungen (Vertragsverzeichnis)

Über die bestehenden Beauftragungen führt <*Stelle bezeichnen*> eine Vertragsübersicht. Der Inhalt der Übersicht ist mit dem Datenschutzbeauftragten abzustimmen.

**Mitgeltende Unterlagen:**

* Vertragsverzeichnis
* Dokumentationen über die Prüfung von Auftragsdatenverarbeitern
* Verträge über eine Datenverarbeitung im Auftrag

1. **Gemeinsam Verantwortliche**

Verfahren und vertragliche Regelungen

Sollen Datenverarbeitungsverfahren in gemeinsamer Verantwortung mit anderen Stellen eingerichtet und betrieben werden, sind die Einzelheiten der Zusammenarbeit, insbesondere die Verpflichtungen zur Wahrnehmung der Rechte der Betroffenen, in einem Vertrag gem. Art. 26 DSGVO zu regeln. Der Datenschutzbeauftragte, ggf. auch der Konzerndatenschutzbeauftragte bzw. Datenschutzkoordinator i. S. v. Nr. 4b dieses Handbuches, ist bei der Gestaltung der vertraglichen Regelungen hinzuzuziehen. Die Tatsache der gemeinsamen Verantwortung ist in der jeweiligen Beschreibung des Verfahrens im Verzeichnis über die Verarbeitungstätigkeiten zu dokumentieren.

**Mitgeltende Unterlagen:**

* Ggf. Verträge

1. **Datenübermittlungen im Konzern und in Drittstaaten**
   1. Konzerninterne Übermittlungen

Konzerninterne Datenübermittlungen sind dem Datenschutzbeauftragten vor der Übermittlung zur Prüfung vorzulegen. Der Datenschutzbeauftragte prüft und beurteilt die Zulässigkeit der Übermittlungen und stellt die Voraussetzungen für Datenübermittlungen fest.

* 1. Übermittlung in Drittstaaten und Vertragsgrundlagen

Bei Übermittlungen in Drittländer prüft der Datenschutzbeauftragte neben der Frage der Zulässigkeit der Übermittlungen auch die besonderen Übermittlungsvoraussetzungen. Vor Abschluss dieser Prüfungen ist eine Übermittlung unzulässig. Bei gesellschaftsübergreifenden bzw. zentralen Verarbeitungsverfahren ist auch der Konzerndatenschutzbeauftragte bzw. Datenschutzkoordinator i. S. v. Nr. 4b dieses Handbuches zu beteiligen.

Der Datenschutzbeauftragte dokumentiert die Prüfungen und berichtet über die Ergebnisse der Prüfung an die Geschäftsleitung. In Zweifelsfällen entscheidet die Geschäftsleitung über die Übermittlungsvorhaben.

**Mitgeltende Unterlagen:**

* Dokumentationen über die Prüfung der Übermittlungsvorhaben
* Ggf. Rechtsgrundlage zur Übermittlung in Drittländer

1. **Zusammenarbeit mit der Aufsichtsbehörde**

Einfache Anfragen und Einholung von Beratungen

Soweit einfache Anfragen und Beratungen unter Wahrung der Anonymität des Unternehmens eingeholt werden (insbesondere durch einen externen Datenschutzbeauftragten), nimmt der Datenschutzbeauftragte diese Kontakte in eigener Verantwortung und unabhängig wahr. Geschehen diese Anfragen im Namen des Unternehmens, ist vorher der zuständige Bereichsverantwortliche zu informieren.

Abgabe von verbindlichen Auskünften und Erklärungen

Verbindliche Auskünfte und Erklärungen werden vor ihrer Abgabe zwischen dem Datenschutzbeauftragten und den betroffenen Fachbereichsverantwortlichen, ggf. mit der Geschäftsleitung, abgestimmt und von den jeweiligen Fachbereichsverantwortlichen erteilt.

Bußgeldverfahren

Der Verkehr mit der Aufsichtsbehörde im Zusammenhang mit Bußgeldverfahren wird von der Geschäftsleitung in Abstimmung mit dem Datenschutzbeauftragten abgewickelt.

Anlaufstelle für die Aufsichtsbehörde

Der betriebliche Datenschutzbeauftragte ist für die Aufsichtsbehörde die Anlaufstelle in allen Datenschutzfragen. Der Datenschutzbeauftragte beteiligt in diesen Angelegenheiten die jeweils betroffenen Fachbereichsverantwortlichen und ggf. die Geschäftsleitung.

1. **Pflege und Versionisierung der Datenschutzdokumente**

Dieses Handbuch und die in diesem Handbuch genannten Datenschutzdokumente sind Pflichtdokumente und unterliegen hinsichtlich der Verwaltung, Pflege und Versionisierung den Regelungen zum Qualitäts- bzw. Dokumentenmanagement.

<*Alternativ*>

Dieses Handbuch und die in diesem Handbuch genannten Datenschutzdokumente sind Pflichtdokumente und sind mit dem Dokumenteneigner, dem Versionsstand und dem Gültigkeitsdatum der Version zu kennzeichnen.

1. **Nachweis der Einhaltung der DSGVO**

Die Datenschutzdokumentation zeigt alle Datenverarbeitungsverfahren der einzelnen Fachbereiche. Die Vollständigkeit und Aktualität der Dokumentation wird vom Datenschutzbeauftragten regelmäßig geprüft. Neu hinzukommende oder wegfallende Verfahren sind von den Bereichsverantwortlichen dem Datenschutzbeauftragten unverzüglich zu melden. Anhand der prozessbasierten Checklisten überprüft und dokumentiert der Datenschutzbeauftragte in den festgelegten Intervallen die Übereinstimmung der Verarbeitungsverfahren mit den Vorgaben in den Datenschutzprozessen und erstellt in Abstimmung mit den jeweiligen Fachbereichsverantwortlichen anhand der Bewertungstabelle eine Bewertung des Standes des Datenschutzes im Unternehmen und berichtet an die Unternehmensleitung. Die Überprüfung der einzelnen Verfahren und rechtlich relevante Feststellungen einschließlich der Ergebnisse von Risikoanalysen und eventuellen Datenschutzfolgenabschätzungen werden im Verzeichnis über die Verarbeitungstätigkeiten dokumentiert.

**Mitgeltende Unterlagen:**

* Datenschutzprozesse
* Checklisten
* Bewertungstabelle
* Verzeichnis über die Verarbeitungstätigkeiten

**Schutzeinstufung von personenbezogenen und betriebswirtschaftlichen**

**Daten**

**Datenverarbeitungsverfahren**

*(Bezeichnung lt. Datenschutz-Verfahrensverzeichnis)*

**Schutzeinstufung**

*(Bei nicht personenbezogenen Daten wird die Schutzeinstufung nach der Tabelle über die betriebswirtschaftlichen Daten vorgenommen.)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Personenkreis** | **Schutzstufe** | | **Anforderungen** |
| **Personenbezogene Daten**  **A bis E** | **Betriebswirt­schaftliche Daten**  **A bis D** |
| Beschäftigte |  |  |  |
| Kunden |  |  |  |
| Lieferanten |  |  |  |
| Sonstige Personen |  |  |  |

**Gesamteinstufung des Verfahrens**

**Personenbezogene Daten:** **Betriebswirtschaftliche Daten:**

**Schutzgrad der Daten**

*(Hier wird nicht nach personenbezogenen bzw. nicht personenbezogenen Daten unterschieden.)*

|  |  |  |
| --- | --- | --- |
| **Schutzziel** | **Schutzgrad**  **1 bis 4** | **Anforderungen** |
| Verfügbarkeit |  |  |
| Integrität |  |  |
| Vertraulichkeit |  |  |
| Authentizität |  |  |
| Revisionsfähigkeit |  |  |

**Legende zur Schutzstufe**

**Schutzstufen personenbezogene Daten**

|  |  |
| --- | --- |
| **Schutzstufe** | **Anforderungen** |
| A | Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z. B. Daten, die die verantwortliche Stelle im Internet oder in Broschüren veröffentlicht bzw. in öffentlich zugänglichen Verzeichnissen zur Verfügung stellt. |
| B | Personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z. B. interne Telefon-Durchwahlnummern, interne Zuständigkeiten. |
| C | Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Stichwort: Beeinträchtigung des Ansehens), z. B. Daten über Vertragsbeziehungen, Höhe des Einkommens, etwaige Sozialleistungen, Ordnungswidrigkeiten. |
| D | Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann (Stichwort: soziale Existenz), z. B. Unterbringung in Anstalten, Straffälligkeit, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Insolvenzen. |
| E | Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (Stichwort: physische Existenz), z. B. Adressen von verdeckten Ermittlern, Adressen von Personen, die mögliche Opfer einer Straftat sein können. |

**Schutzstufen betriebswirtschaftliche Daten**

|  |  |
| --- | --- |
| **Schutzstufe** | **Anforderungen** |
| A | Die betriebswirtschaftlichen Daten sind frei zugänglich, müssen aber richtig sein. |
| B | Interne betriebswirtschaftliche Daten. Ein Missbrauch verursacht keine besondere Beeinträchtigung der betrieblichen Funktion oder der Umweltbeziehungen des Unternehmens. |
| C | Ein Missbrauch von betriebswirtschaftlichen Daten kann die betriebliche Funktion, die Umweltbeziehungen oder das Ansehen des Unternehmens erheblich beeinträchtigen. |
| D | Ein Missbrauch kann die finanzielle oder marktwirtschaftliche Situation oder die Existenz eines Unternehmens erheblich beeinträchtigen. |

**Legende zum Schutzgrad**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schutz­grad** | **Verfügbarkeit**  Daten müssen jederzeit zur Ver­fügung stehen und ordnungs­gemäß verarbeitet werden können. | **Integrität**  Daten müssen wäh­rend der Verarbei­tung unversehrt, voll­ständig und aktuell bleiben. | **Vertraulichkeit**  Daten müssen vor unbefugter Kenntnis­nahme geschützt werden. | **Authentizität**  Daten müssen ihrem Ursprung zugeordnet werden können. | **Revisionsfähigkeit**  Entwicklung, Ein­satz, Wartung, Administra­tion und Anwendung des Verfahrens und Ver­arbeitung der Daten müssen nachvollziehbar sein. |
| **1** | Allgemeine Ver­fügbarkeit:  Keine zeitkriti­schen Verfahren, keine besonde­ren Anforderun­gen an die Ver­fügbarkeit bzw. Wiederher­stel­lung der Verfüg­barkeit. Die Wie­derherstellung unterliegt den allgemeinen Regeln zur Datensicherung. | Ungesicherte Integrität:  Die Daten unter­liegen keinen besonderen Maß­nahmen zur Siche­rung der Integrität. | Öffentlich:  Es bestehen keine Anforderungen an die Vertraulichkeit. | Eine Nach­weis­barkeit der Authentizität ist nicht gefordert. | Keine Anforderun­gen an die Revisi­ons­­fähigkeit des Datenverarbei­tungs­verfahrens. |
| **2** | Definierte Ver­fügbarkeit:  Zeitkritische Verfahren mit definierten An­forderungen an die Verfügbarkeit bzw. Wiederher­stellung der Verfügbarkeit. Ein Sicherungs- und Rekonstruk­tionskonzept muss vorhanden sein. | Geschützte Integrität:  Der Verlust der Integrität kann zu einer Störung der betrieblichen Funktionen führen.  In den Verfahren müssen Vorkeh­rungen zum Schutz der Daten vor unbefugten Veränderungen und Datenverlus­ten eingerichtet sein, z. B. ein Be­rechtigungs­­­sys­tem, Passwort­schutz, Schreib­sperre etc. | Intern:  Die Informationen dürfen nur intern verwendet und nicht an Dritte weitergegeben werden. | Kontrollierbare Authentizität:  Der Verlust der Authentizität kann zu einer Störung der betrieblichen Funktionen führen. Es muss nach­voll­ziehbar sein, dass nur berech­tigte Personen die Daten erzeugt bzw. eingestellt und ggf. geän­dert haben, z. B. durch Berech­tigungs­profile. | Allgemeine Anforderungen:  Es bestehen keine erhöhten Anforde­rungen an die Revi­sionsfähigkeit.  Do­kumentation und Nachvollziehbarkeit der Datenverarbei­tungsverfahren und der Datenverarbei­tung unterliegen den allgemeinen Rege­lungen. |
| **3** | Hoch verfügbar:  Businesskriti­sche Daten und Verfahren mit besonders ho­hen Ansprüchen an Verfügbarkeit und Wiederher­stellung. Ein Notfallplan und ein Sicherungs- und Rekonstruk­tionskonzept müssen vorhan­den sein. | Nachprüfbare Integrität:  Der Verlust der Integrität kann empfindliche Schäden verursa­chen. In den Ver­fahren müssen Vorkeh­rungen zum Nachweis des Schutzes der Integrität vorgese­hen sein, z. B. Protokollierung von Änderungen, Prüfsummen etc. | Vertraulich:  Die Daten sind nur einem bestimmten oder bestimmba­ren Personenkreis zugänglich. | Beweisbare Authentizität:  Der Verlust der Authentizität kann zu emp­find­lichen Schä­­den füh­ren. Es muss nach­voll­zieh­bar sein, wer die Daten wann erzeugt bzw. eingestellt und ggf. geän­dert hat, z. B. durch Protokol­lierun­gen. | Erhöhte Anforderungen:  Die Nachvollzieh­barkeit und Prüfbar­keit der Verfahren und der Datenverar­beitung unterliegen erhöhten Anforde­rungen. Entwick­lung, Testung, Frei­gabe, Administra­tion, Anwendung der Verfahren, die Integ­rität der Programme und die Verarbei­tung der Daten müssen dokumen­tiert und nachvoll­ziehbar sein. |
| **4** |  | Signierte Integrität:  Die Integrität der Daten muss beweisbar sein, z. B. bei Urkunden oder elektronischen Rechnungen.  Die Integrität der Daten muss durch eine qualifizierte elektronische Signatur oder ein vergleichbar sicheres Verfahren gewährleistet sein. | Streng vertraulich:  Die Daten sind nur einem namentlich festgelegten Personenkreis zugänglich. | Signierte Authentizität:  Die Authentizität muss unverfälschbar nachgewiesen werden können, z. B. bei Urkunden. Der Nachweis muss durch eine elektronische Signatur oder ein vergleichbar sicheres Verfahren geführt werden können. | Höchste Anforderungen:  Die Nachvollziehbarkeit und Prüfbarkeit der Verfahren und der Datenverarbeitung unterliegen nochmals erhöhten Ansprüchen. Die Unveränderbarkeit von Programmen, Dokumentationen, Administrations- und Verarbeitungsprotokollen und sonstigen Aufzeichnungen sowie die Nachvollziehbarkeit der Verarbeitung der Daten muss gegeben und die Gewährleistung der Revisionsfähigkeit in einem Konzept beschrie­­­ben sein. |