Externer
Datenschutzbeauftragter

Vorgehen, Maßnahmen und Betreuung

PRIOLAN®
DATENSCHUTZ & IT-SICHERHEIT

Unser Vorgehen

Als Datenschutzbeauftragte ist es unsere Aufgabe, auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken. Zu diesem Zweck führen wir im Rahmen einer Dokumentenreview, durch Gespräche und Vor-Ort Begehung eine Bestandsaufnahme durch. Diese Informationen werten wir in der Konzeptionsphase rechtlich und sicherheitstechnisch aus, erstellen erforderliche Dokumente und arbeiten Lösungsvorschläge aus. Im weiteren Verlauf unterstützen wir Sie bei der Umsetzung und überwachen fortlaufend die Prozesse. Aus Gründen eines reibungslosen Gangs der Geschäftsabläufe und zur gleichmäßigen Verteilung der Kosten hat sich in der Praxis häufig eine schrittweise Bestandsaufnahme bei gleichzeitiger Umsetzung akut anstehender Maßnahmen bewährt.

Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen im Unternehmen

Das Aufgabenfeld des Datenschutzes ist weit gefächert. Welche Maßnahmen zu ergreifen sind, ergibt sich aus den Anforderungen des Bundesdatenschutzgesetzes und dem Ergebnis der IST-Analyse. Die Maßnahmen lassen sich vielfach parallel in Angriff nehmen, unterscheiden sich jedoch in ihrer Umsetzungsdauer. Um Ihnen einen Überblick über die Arbeit des Datenschutzbeauftragten zu geben, sollen die Maßnahmen untergliedert nach kurzfristigen, mittelfristigen und langfristigen Maßnahmen nachfolgend im Einzelnen vorgestellt werden.

Kurzfristige Maßnahmen

- **Verpflichtung der Mitarbeiter auf das Datengeheimnis**
  - Schriftliche Verpflichtung der bei der Verarbeitung personenbezogener Daten tätigen Personen auf das Datengeheimnis gemäß § 5 BDSG bzw. Überprüfung der bestehenden Formulare.
  - Ggf. schriftliche Verpflichtung der bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten tätigen Personen auf das Fernmeldegeheimnis gemäß §88 TKG.
- **Erste Tätigkeiten**
  - Veröffentlichung eines ersten Artikels in der Betriebszeitung oder im Intranet über die Notwendigkeit der Beachtung datenschutzrechtlicher Vorgaben im Unternehmen.
  - Halten eines kurzen Vortrages über die Notwendigkeit der Beachtung datenschutzrechtlicher und IT-sicherheitsrelevanter Vorgaben im Unternehmen.

Mittelfristige Maßnahmen

- **Entwicklung eines Schulungs- und Informationskonzepts**
  - Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen ggf. anhand einer Zielgruppenorientierung
    - Geschäftsleitung, Führungskräfte, besondere Funktionsgruppen, Mitarbeiter, ggf. Fremdpersonal bzw. Auftragsdatenverarbeiter (bspw. externe IT-Dienstleister) durch geeignete Maßnahmen über die Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz und vertraut machen mit den jeweiligen besonderen Erfordernissen des Datenschutzes nach § 4g Abs. 1 Satz 3 Nr. 2 BDSG (bspw. durch Online-Selbstschulungen; persönliche Gruppenschulungen, um zu gewährleisten, dass jeder Mitarbeiter die für ihn relevanten Datenschutzregeln kennt und beachtet.
    - Dokumentation der Schulungsteilnahme, Lernerfolgskontrolle.
  - Ggf. gesonderte Schulung des Betriebsrats und der Personalabteilung über die besonderen Erfordernisse des Arbeitnehmerdatenschutzes.
  - Einsatz unterschiedlicher Medien wie Merkblätter oder Broschüren, Veröffentlichung von Hinweisen und Fachbeiträgen zu datenschutzrechtlichen Fragen allgemeiner oder gruppenspezifischer Art sowie zu besonderen Vorkommnissen im Intranet oder am „Schwarzen Brett".
- **Errichtung interner und externer Verfahrensverzeichnisse**
  - Führen des internen Verfahrensverzeichnisses nach § 4g Abs. 2 Satz 1 BDSG sowie des externen Verfahrensverzeichnisses nach § 4g Abs. 2 Satz 2 BDSG.
  - Ggf. Einsatz eines entsprechenden Software-Tools zur zweckentsprechenden Erfassung, Verwaltung und Auswertung der vom BDSG vorgeschriebenen Informationen über ein Verarbeitungsverfahren.
- **Durchführung von Vorabkontrollen**
  Vornahme von Vorabkontrollen nach § 4d Abs. 5 und Abs. 6 BDSG bei solchen automatisierten Verarbeitungen personenbezogener Daten, welche besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen.
- **Erarbeitung betriebsinterner Standards zum Datenschutz**
  - Entwicklung, Implementierung und Weiterentwicklung von betriebsinternen Richtlinien zum Datenschutz (betriebsinterne Standards zum Umgang mit personenbezogenen Daten, Nutzung der betrieblichen IT-Infrastruktur, Nutzung der Telefon-, Fax-, Internet- und E-Mail-Dienste, Zugang zu Betriebsräumen, Verwendung von Passwörtern, Verschlüsselung von Daten, Entsorgung von Datenträgern etc.), entweder in Form von verbindlichen Dienstanweisungen oder bei Vorhandensein eines Betriebsrates in Form von Betriebsvereinbarungen in Zusammenarbeit mit den betroffenen betriebsinternen Stellen (Personal-, IT-, Rechts-, ggf. Vertriebs- / Marketing-, Einkaufsabteilung und Betriebsrat).
  - Bereitstellung entsprechender Entwürfe.
  - Koordinierung der Maßnahmen mit Management, Personalabteilung und Betriebsrat.
  - Durchführung von Kontrollen.
- **Sicherstellung erforderlicher Maßnahmen aus Anlass einer Datenverarbeitung im Auftrag resp. einer Funktionsübertragung**
  - Ermittlung datenschutzrechtlichen Handlungsbedarfes infolge einer Auftragsvergabe an (konzern-) interne oder externe Dienstleister nach § 11 BDSG.
  - Bereitstellung entsprechender Vertragsentwürfe nach § 11 Abs. 2 Satz 2 BDSG.
  - Gestaltung entsprechender Weisungen nach § 11 Abs. 3 BDSG.
  - Durchführung von Kontrollen § 11 Abs. 2 Satz 4 BDSG.
  - Regelungen zur Funktionsübertragung nach § 28 Abs. 5 BDSG.

- **Grenzüberschreitende Datenübermittlungen**
  - Ermittlung der datenschutzrechtlichen Zulässigkeit und des Handlungsbedarfes nach §§ 4b und 4c BDSG (Zulässigkeitsvoraussetzungen EU/EWR/Drittstaaten, Beurteilung des Angemessenheit des Datenschutzniveaus, Genehmigungsverfahren der Aufsichtsbehörden, Datenübermittlung im Konzerngefüge, Besonderheiten bei Mitarbeiterdaten, Grenzüberschreitende DViA, „Offshoring", „Nearshoring").
  - Bereitstellung entsprechender Garantien bei einer Datenübermittlung in einen Drittstaat ohne angemessenes Datenschutzniveau nach § 4c Abs. 2 BDSG (z.B. Vertragslösung, Standardvertragsklauseln der EU-Kommission, Safe Harbor Principles, Codes of Conduct).
- **Sicherstellung erforderlicher Maßnahmen nach dem TKG und TMG**
  - Im Innenverhältnis
    - Dienstliche / private Nutzung des Telefon-, E-Mail-, Internet- und Intranet-Dienstes.
    - Social Media Richtlinie, Mitarbeiterdaten im Internet / Intranet.
    - Filterung von E-Mails.
  - Im Außenverhältnis
    - Webauftritt, Impressumspflichten / Anbieterkennzeichnung nach § 4 Abs. 3 BDSG, §§ 5,6 TMG.
    - Konformität der Inhalte, insbesondere der Texte, Fotos, Illustrationen und Sounds sowie des Layouts der Website selbst mit dem UrhG.
    - Konformität des Domainnamens mit Namens- oder Markenrechten Dritter.
    - Kontrolle der verlinkten Seiten auf offensichtlich rechtswidrige Inhalte, um eine Haftung für Fremdinhalte zu vermeiden.
    - Bereitstellung einer Datenschutzerklärung bzw. „Privacy Policy" (beinhaltet möglichst detaillierte Informationen über die Art, die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten, insbesondere deren Weitergabe an Dritte, die Dauer der Speicherung und die Möglichkeit der Löschung sowie Fragen zur Datensicherheit: Unterrichtung des Nutzers über die Verarbeitung seiner personenbezogenen Daten nach § 13 Abs. 1 TMG).
    - Hinweise des Nutzers auf Widerspruchsrechte nach § 13 Abs. 3 TMG.
    - Beachtung der Erfordernisse einer Einwilligung und des Rechts auf Widerruf nach § 13 Abs. 2 TMG.
    - Unterrichtung über technisch-organisatorische Vorkehrungen nach § 13 Abs. 4 TMG.
    - Sicherstellen des Rechts auf Auskunft nach § 13 Abs. 7 TMG, 6a Abs. 3 BDSG.
    - Hinweis auf das Setzen von Cookies und Google Analytics, datenschutzgerechte Gestaltung von Eingabeformularen.
    - Beachtung datenschutz- und wettbewerbsrechtlicher Erfordernisse bei Newslettern, Direkt- und E-Mail-Marketing.
    - Gegebenenfalls Beachtung jugendschutzrechtlicher Vorgaben.
    - Informationspflichten gegenüber Verbrauchern im Fernabsatz nach §§ 312b ff BGB.
    - Pflichten im elektronischen Geschäftsverkehr nach § 312d BGB.

- **Organisation der Betroffenenrechte**
  Durch Implementierung organisatorischer Maßnahmen sind insbesondere folgende Betroffenenrechte betriebsinterner Art (arbeitnehmerbezogene Datenverarbeitung) sowie betriebsexterner Art (kunden-, lieferanten-, auftragnehmerbezogene Datenverarbeitung) sicherzustellen:
  - Unterrichtung nach § 4 Abs. 3 BDSG.
  - Benachrichtigung gem. § 33 BDSG.
  - Auskunft gem. § 34 BDSG.
  - Berichtigung, Löschung und Sperrung gem. § 35 BDSG.
  - Widerspruch gem. § 28 Abs. 4 BDSG.
- **Beratungstätigkeit**
  Beratung (bspw. in Form von persönlichen Gesprächen, Telefonaten, E-Mails, Briefen, Stellungnahmen, Gutachten) in Datenschutzfragen (bspw. allgemeine Fragen zum Datenschutzrecht; praktische Fragen zur Umsetzung von Rechtsvorschriften; Anforderungen der Aufsichtsbehörden; Fragen zur arbeitsplatz-, arbeitnehmer-, kunden-, lieferanten-, auftragnehmerbezogenen Datenverarbeitung; datenschutzgerechter Internetauftritt; Outsourcing [Datenverarbeitung im Auftrag, Funktionsübertragung]; datenschutzkonforme Datenübermittlung ins Ausland) von:
  - Geschäftsführung, Management bzw. Leitungs- und Planungsgremien (insbesonders die Abteilungen)
    - IT (bspw. Implementierung der technischen und organisatorischen Maßnahmen entsprechend der Anlage zu § 9 BDSG; Erstellung von Datenschutz- und IT-Sicherheitskonzepten; elektronische Archivierung),
    - Personal (s. Ausführungen zu Betriebsrat),
    - Vertrieb / Marketing (bspw. Customer Relationship Management - CRM, Kundenbindungsprogramme, personenbezogene Marketing-Aktivitäten, Einwilligungsmanagement, werbliche Ansprache)
  - Betriebsrat
    - Datenschutzpflichten des Betriebsrates,
    - Rechtsgrundlagen und aktuelle Rechtsprechung zur Zulässigkeit der Verarbeitung von Mitarbeiterdaten (Mitbestimmungsrechte, Informationsrechte, Kontrollbefugnisse),
    - Rechte der Mitarbeiter, datenschutzgerechte Gestaltung von Personalinformationssystemen, Mitarbeiterdatenschutz im Call Center,
    - Kontrolle von Internet- und E-Mail-Einsatz,
    - Personaldaten im Internet, Videokontrolle, Telearbeit,
    - Datenflüsse bei Wechsel des Arbeitgebers (bspw. Arbeitgeberauskunft, Betriebsveräußerung),
    - Assistenz bei der Konzeptionierung von Betriebsvereinbarungen mit Berührungspunkten zur arbeitsplatz- und arbeitnehmerbezogenen Datenverarbeitung.
  - Belegschaft, Betriebsarzt, Kunden, Auftragnehmern, Lieferanten, Betroffenen.
- **Vertretung nach außen**
  Vertretung des Unternehmens bzw. Agieren als Ansprechpartner gegenüber externen Stellen (bspw. Aufsichtsbehörden, Betroffene, Kunden, Auftragnehmer und Lieferanten) in datenschutzrechtlich relevanten Fragestellungen und Steuerung aller damit zusammenhängenden Kontakte. Vertretung des Unternehmens in Fachgremien.
- **Tätigkeit bei besonderen Vorkommnissen**
  - Einleitung vorbereitender Maßnahmen bei angekündigtem, aufsichtsbehördlichem Besuch.
  - Führung der Gespräche und der Verhandlungen auf Unternehmensseite.
  - Beratende Tätigkeit bei Vorgängen gegenüber den Strafverfolgungs- und Sicherheitsbehörden sowie der Bundesnetzagentur, soweit die Vorgänge einen Bezug zum Daten- oder Fernmeldegeheimnis aufweisen.
  - Telefonische Auskunft und Beratung in Akutfällen.
  - Planung und Durchführung eines Datenschutzaudits.

Langfristige Maßnahmen

- **Errichtung eines Datenschutzkonzeptes**
  Unter einem Datenschutzkonzept ist eine strukturierte Analyse möglicher Gefahren- und Schadenszenarien und darauf aufbauender Schutzmaßnahmen zu verstehen. Die Schutzmaßnahmen werden unter Berücksichtigung sämtlicher der in der Anlage zu § 9 BDSG erläuterten einzelnen technisch-organisatorischen Maßnahmen getroffen. Das Konzept muss eine Revisionssicherheit ermöglichen. Kernbestandteile eines Datenschutzkonzeptes sind regelmäßig:
  - Bestandsaufnahme
  - Schutzbedarfsfeststellung
  - Risiko-/Gefahrenanalyse
  - Maßnahmenauswahl
  - Verhältnismäßigkeits-/Wirtschaftlichkeitsbetrachtung
  - Festlegung von Implementierungszeitrahmen und Verantwortlichkeiten
  - Umsetzung und fortlaufende Kontrolle
  - Evaluierung der Resultate und ggf. Nachbesserung bzw. Neukonzipierung zutreffender Maßnahmen
- **Implementierung eines Datenschutzmanagementsystems**
  - Aufbau eines Kontrollsystems
    Um die Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, nach § 4g Abs. 1 Satz 3 Nr. 1 BDSG sicherzustellen und um die unverzügliche Behebung von datenschutzrechtlichen Schwachstellen zu gewährleisten, ist per Organisationsanweisung sicherzustellen, dass der DSB rechtzeitig über die automatisierte Verarbeitung personenbezogener Daten unterrichtet wird.

- Aufbau eines Dokumentationssystems
  Um den datenschutzrechtlichen Erfordernissen zum Nachweis der rechtlichen Zulässigkeit und der Zweckbindung nach §§ 4, 28, 29, 30, 31 BDSG und den erforderlichen technisch-organisatorischen Maßnahmen nach § 9 BDSG sowie der nach § 7 BDSG gebotenen Sorgfalt zu entsprechen, ist eine hinreichende Dokumentation sicherzustellen. Ferner sind die Aktualität der Dokumentation und ein rascher Zugriff darauf sicherzustellen.
- Einbindung in betriebliche Prozesse der Compliance und der Qualitätssicherung
  - Identifikation datenschutzrelevanter Schnittstellen.
  - Risikomanagement (Bewertung und Gewichtung der Risiken nach rechtlichen, wirtschaftlichen, unternehmenspolitischen, technischen und organisatorischen Kriterien).
  - Koordinierung der Aktivitäten und Bilden einer gemeinsamen Schnittstelle mit Internem Kontrollsystem (IKS), um den Überwachungs- und Dokumentationspflichten anderer gesetzlicher Erfordernisse im Unternehmen zu entsprechen (z.B. „Compliance"-Anforderungen im Hinblick auf IT-Sicherheitsaspekte nach KonTraG, SOX, Basel II).
  - Koordinierung der Anforderungen des Datenschutzes mit solchen der Qualitätssicherung aus anderen laufenden und geplanten betrieblichen Prozessen (bspw. Personalplanung und –entwicklung, IT, Marketing, Verkauf, Einkauf, Auftragsabwicklung / Projektabwicklung, Hausverwaltung / Wartung / Service, Qualitätsmanagement, Reklamationsbearbeitung, Vertrags- / Dokumentenmanagement, Finanzbuchhaltung, Controlling / Auditierung, Mahnwesen/Inkasso, Internet-Auftritt), um eine integrierte Lösung zu erreichen (Synergieeffekte).
  - Zusammenarbeit mit anderen Kontrollstellen (bspw. Revision, externe Prüfer, Auditoren).
- Implementierung DS-Management-Software
  Die Erfordernisse aus den vorstehenden Punkten können einträglich durch den Einsatz eines Software-Tools abgedeckt werden, mit dem entsprechende Daten dezentral von Mitarbeitern erfasst und dem DSB in einer zentralen Datenbank, zur Auswertung und zum Erkennen von Handlungsbedarf zur Verfügung gestellt werden.
- Unterstützung bei der Erstellung eines Datenschutzbudgets.
- Bedarfseinschätzung und –planung für Sachmittel und für die Inanspruchnahme von internen und externen Dienstleistungen.

Koordination und Kontrolle der einzelnen Konzerngesellschaften bei Konzernbeauftragung

- Entwicklung einer einheitlichen Datenschutzphilosophie mit grundlegenden Zielvorgaben, die als Kontrollmaßstab für alle Konzerngesellschaften gelten und die datenschutzrechtlichen Interessen der Einzelgesellschaften berücksichtigen.
- Entwicklung einer für alle Unternehmen einheitlichen Datenschutzstrategie zur Erreichung der datenschutzrechtlichen Zielvorgaben.
- Ausgestaltung der Datenschutzorganisation mit Festlegung der zu treffenden, baulichen, organisatorischen, personellen und technischen Einzelmaßnahmen zur Umsetzung der Strategie im Konzern und in den einzelnen Gesellschaften.
- Betreuung, Anweisung und Kontrolle der für den Datenschutz verantwortlichen Mitarbeiter.

Tätigkeitsbericht

- Vorlegen eines Tätigkeitsberichtes zum Ende eines jeden Geschäftsjahres gegenüber der Unternehmensleitung
  - Wesentliche Entwicklung gegenüber der Vorperiode.
  - Datenschutzmaßnahmen (Tätigkeiten im Berichtszeitraum, Planung für den kommenden Berichtszeitraum, Arbeitnehmerdatenschutz, Datenverarbeitung im Auftrag / Funktionsübertragung).
  - Datensicherheit/IT-Sicherheit
  - Qualifikation DSB
  - Anfragen/Beschwerden zum Datenschutz.

PRIOLAN bietet folgende LEISTUNGEN an.

DATENSCHUTZ

- Externer Datenschutzbeauftragter
- Datenschutzaudit
- ERFA-Kreis
- Mitarbeiterschulungen
- Informationsveranstaltungen

IT- SICHERHEIT

- ISO/IEC 27001
- IT-Security Audit
  - Hacker Angriffe aus dem Internet
  - Interne Blackbox-Tests
  - Interne Whitebox-Tests
  - Social Hacking
  - Organisatorische Tests
  - Informationsveranstaltungen
- Sicherheitskonzepte und Umsetzung

PRIOLAN GMBH

GOTTLIEB-DAIMLER-STRASSE 9 · 74076 HEILBRONN
T +49 (0)7131 2628 0 · F +49 (0)7131 2628 300
INFO@PRIOLAN.DE · WWW.PRIOLAN.DE

PRIOLAN®
DATENSCHUTZ & IT-SICHERHEIT