# L c enh fter Dat n chutz

## Handbuch zur Datenschutzeinführung

GREAT OAK
DATENSCHUTZ

# Datenmiss-brauch die Stirn bieten

## mit fachmännischer Unterstützung

Was sich wo findet:

Sehr geehrter Leser, sehr geehrte Leserin,

diese Broschüre soll Ihnen helfen, die Fachbegriffe im Datenschutz besser einzuordnen. Sie haben zusammen mit dieser Broschüre ein Angebot über Datenschutzdienstleistungen aus unserem Haus erhalten. In diesem Angebot werden einige Fachbegriffe benutzt, da nur so die angebotene Leistung korrekt beschrieben werden kann. Würden wir sie alle im Angebotstext erläutern, würde es den Rahmen eines vernünftigen Angebotes sprengen. Wir haben uns deshalb für die Auslagerung in eine gesonderte Broschüre entschieden.
Damit Sie nicht erst mühsam im Internet nach Begriffen suchen müssen, die Sie vielleicht noch nicht kennen, haben wir Ihnen zu den wichtigsten Begriffen eine Erklärung beigefügt. Sie können also, wenn Sie es möchten, jederzeit etwas nachschlagen.
Gerne können Sie uns auch Ihre Fragen zum Angebot direkt stellen, wir freuen uns auf ein Gespräch mit Ihnen.

Auf eine gute zukünftige Zusammenarbeit,

Florian Schirm
Geschäftsführer

# Great Oak

## Unsere Leistungen beim Projekt „Einführung Datenschutz“

Falls Sie Ihren Datenschutz bisher noch nicht an die Anforderungen der Datenschutzgrundverordnung (DSGVO) angepasst haben oder das Thema Datenschutz neu angehen, sind einige grundlegende Maßnahmen umzusetzen, die nur einmalig anfallen. Die Tätigkeiten, die dieses Projekt umfassen, sind:

- Ersteinweisung der beteiligten Mitarbeiter
- Einweisung, Unterstützung und Begleitung der Verantwortlichen bei der Dokumentation der Verarbeitungstätigkeiten (Verarbeitungsübersicht)
- Falls gesetzlich erforderlich, Unterstützung des jeweiligen Verantwortlichen bei der Durchführung einer Datenschutzfolgenabschätzung (Risikoanalyse für eine bestimmte Datenverarbeitung)
- Erstprüfung der Angemessenheit der bisher etablierten technischen und organisatorischen Maßnahmen zum Schutz der Daten
- Gemeinsame Ausarbeitung einer Datenschutzrichtlinie mit dem Verantwortlichen, um die organisatorischen Datenschutzaspekte für Ihre Mitarbeiter zu regeln
- Ausarbeitung einer IT-Sicherheitsrichtlinie in Zusammenarbeit mit den Verantwortlichen und der IT-Abteilung bzw. dem IT-Dienstleister, zur Regelung der technischen Aspekte im Bereich der digitalen Datenverarbeitung
- Begleitung der Implementierung eines Löschkonzepts
- Analyse der Auftragsverarbeitungen und der dazu bestehenden Vertragsverhältnisse
- Bereitstellung und ggf. Anpassung von Vorlagen zur Erfüllung der gesetzlich vorgeschriebenen Informationspflichten
- Erarbeitung des Dokuments „Einwilligungen durch die Betroffenen“ für relevante Datenverarbeitungen

# Grafische Darstellung Ablauf Datenschutz-Projekt

# Datenschutz-Managementsystem

Mitarbeiter, die sich mit dem Thema Datenschutz beschäftigen müssen, fragen sich oftmals, wie sie die ganzen Datenschutzdokumentationen erfassen, speichern und pflegen sollen, sowie die vielen vorgeschriebenen Tätigkeiten protokollieren können. Hierbei stehen Sie nicht allein da, sondern können sich durch spezielle Software unterstützen lassen. Auf den ersten Blick scheint eine solche Software nur weitere Kosten zu verursachen, aber im täglichen Umgang mit dem Thema Datenschutz spart Ihnen eine solche Software sehr viel Zeit und Mühe, was sich in geringerem Personaleinsatz niederschlägt. Zudem haben Sie alle relevanten Daten an einem Ort und können so bei Kontrollen oder anderen Problemen direkt auf alle notwendigen Informationen zugreifen, um negative Konsequenzen oder sogar Bußgelder zu vermeiden.

Außer bei sehr kleinen Unternehmen, die auch mit Tabellen und PDFs gut versorgt sind, empfehlen wir Ihnen unbedingt die Verwendung einer solchen Software.
In unserem Angebot zur Übernahme der Tätigkeit als Datenschutzbeauftragter finden Sie eine gesonderte Position für eine solche Software, die von uns betrieben wird. Hierbei bekommen Sie einen eigenen Mandanten in der Software auf einem unserer Server. Möchten Sie Ihre Dokumentationen lieber im eigenen Haus haben, können Sie die Software auch direkt in Ihrer IT-Infrastruktur betreiben. Dies verursacht jedoch in der Regel um ein Vielfaches höhere Kosten, da Sie bei uns das Grundpaket schon inklusive haben und nur den Mandanten, sowie einen Anteil an der Wartung des Systems zahlen müssen.

# Verzeichnis von Verarbeitungstätigkeiten (Verfahrensverzeichnis)

Beim Verzeichnis von Verarbeitungstätigkeiten (ehemals Verfahrensverzeichnis) handelt es sich um eine Beschreibung aller langfristig stattfindenden Prozesse, bei denen personenbezogene Daten verarbeitet werden. Solche Verfahren sind beispielsweise das Bewerbungsmanagement, die Abrechnung von Leistungen, die Erfassung von IP-Adressen durch die Webseite, das Führen einer Kundendatei usw.
Das Verzeichnis von Verarbeitungstätigkeiten muss grundsätzlich von jedem geführt werden, der nicht nur rein privat Daten verarbeitet. Hierzu zählen neben Unternehmen auch Praxen, Apotheken, kirchliche Einrichtungen, Kleinstgewerbe und alle Vereine.

!

Für Unternehmen und Einrichtungen ab 250 Mitarbeitern und für jede Verarbeitung besonders sensibler Daten, wie beispielsweise Gesundheitsdaten, Religionsdaten usw. (Definition in Art. 9 Abs. 1 DSGVO), gilt diese Pflicht auch für nicht dauerhafte Verarbeitungen.

Die Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten sollte aber nicht nur als bürokratische Pflicht verstanden werden. Das Verzeichnis und seine Erstellung bieten die Chance, herauszufinden, wo und wie Daten im eigenen Hause wirklich verarbeitet werden. Oftmals gibt es bei der Erstellung überraschende Einblicke. Zudem kann mittels dieses Verzeichnisses auch die zukünftige Datenverarbeitung in geregeltere Bahnen gelenkt werden.

Was können wir für Sie übernehmen:
- Einweisung in die Erfassung von Verarbeitungen (inkl. Beispielverarbeitungslisten)
- Begleitung bei der Verschriftlichung der Verarbeitungen (optional)
- Assistentenbasierte Eingabe über unser Datenschutzmanagementsystem
- Prüfung der eingegebenen Verfahren auf Vollständigkeit und Plausibilität
- Abgleich von IST-Zustand und im Verzeichnis beschriebenem Zustand bei jährlichen Audits
- Anpassung von Verarbeitungsbeschreibungen bei Änderungen

Wobei ist Ihre Tatkraft erforderlich:
- Festlegen der Verarbeitungen
- Beschreibung der Verarbeitungen

# Aufbau des Verzeichnisses von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten muss schriftlich geführt werden, wobei es aber in elektronischer Form vorliegen darf. Der Mindestinhalt muss Folgendes umfassen:

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters
- Bei gemeinsamer Datenverarbeitung Name und Kontaktdaten der gemeinsamen Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung (Beschreibung des Grundes, warum die Daten verarbeitet werden)
- Beschreibung der Kategorien betroffener Personen
- Beschreibung der Kategorien verarbeiteter Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- Fristen für die Löschung der verschiedenen Datenkategorien
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen
- Ggf. Informationen zu Empfängern im außereuropäischen Ausland
- Zudem sollten die Eingaben noch um Folgendes ergänzt werden:
  - Kurze Beschreibung der Verarbeitungen
  - Angabe der Rechtsgrundlagen
  - Interne Zugriffsrechte und Weiterleitungen

§

Geregelt wird die Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten in Art. 30 DSGVO. Ein fehlendes oder unvollständiges Verzeichnis kann gem. Art. 83 Abs. 4 lit. a DSGVO mit einem Bußgeld geahndet werden. Zudem dient das Verzeichnis als Teil der nach Art. 5 Abs. 2 DSGVO geforderten Rechenschaftspflicht.

# Datenschutzfolgenabschätzung

Ist eine Datenverarbeitung besonders risikoreich oder kommen neue Technologien (z.B. Cloudanwendungen) zum Einsatz, löst dies für den Verantwortlichen eine Pflicht zur Durchführung einer Datenschutzfolgenabschätzung aus. Hierzu zieht er den betrieblichen Datenschutzbeauftragten mit zu Rate. (Bei einer Pflicht zur DSFA muss immer ein Datenschutzbeauftragter bestellt sein.)
Eine DSFA muss schriftlich und systematisch aufgebaut erfolgen. Sie umfasst:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge im Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen,
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die relevanten Datenschutzgesetze eingehalten werden.

Die Datenschutzfolgenabschätzung muss erneut durchgeführt werden, wenn sich Sachverhalte der Datenverarbeitung oder die Rahmenbedingungen ändern. Mindestens einmal jährlich sollten Sie prüfen, ob dies der Fall ist.

§

Geregelt wird die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung in Art. 35 DSGVO, § 35 KDG und § 34 DSG-EKD.


iM dsCHunGel
der GeseTZli-
chEn VoRgaBEn
behalten wir den
Überblick

# Richtlinien

Bei der schriftlichen Regelung der TOMs (Technisch-Organisatorische-Maßnahmen) bietet sich eine Aufteilung der Regelungen in zwei Richtlinien an, um den technischen Teil vom organisatorischen zu trennen.

**Datenschutzrichtlinie**
Aus der Zusammenfassung aller Arbeitsanweisungen und Vorgaben für das datenschutzkonforme Verhalten an einem Ort ergibt sich die Datenschutzrichtlinie. Ergänzend sollten hier Sonderfälle beschrieben werden, die nicht alltäglich vorkommen. Zudem bietet es sich an, den Aufbau des Datenschutzes und die verfolgten Ziele an dieser Stelle zu definieren. Die Datenschutzrichtlinie gibt den Mitarbeitern Orientierung und Sicherheit im Umgang mit personenbezogenen Daten und dient Ihnen als Nachweis der Einhaltung vorgeschriebener Verhaltensweisen.

**IT-Sicherheitsrichtlinie**
Mit der IT-Sicherheitsrichtlinie definieren Sie ein technisches Schutzziel für Ihre Infrastruktur. Sie ist keine Beschreibung des Ist-Zustandes, sondern definiert den Soll-Zustand, der in naher Zukunft erreicht werden soll. Zudem legt sie fest, wie neue Infrastrukturen anzuschaffen und zu installieren sind. Auch spezielle Vorgaben für die Konfiguration von Soft- und Hardware werden hier festgelegt. Sie stellt sicher, dass Ihre technischen Maßnahmen zum Schutz Ihrer Daten planvoll und in die richtige Richtung erfolgen. Gleichzeitig stellt sie auch ein motivierendes Arbeitsinstrument für Ihre IT-Betreuer dar.

# Technisch-Organisatorische-Maßnahmen (TOMs): Technische Aspekte

Zum Schutz der personenbezogenen Daten vor missbräuchlicher Nutzung und Verlust schreibt der Gesetzgeber vor, dass vom Verantwortlichen technische und organisatorische Maßnahmen zu ergreifen sind, um die Eintrittswahrscheinlichkeit eines solchen Vorfalls zu minimieren.
Zu den technischen Maßnahmen zählen beispielsweise:

- Verschlüsselung aller Datenbestände
- Verschlüsselte E-Mail-Kommunikation und verschlüsselter Datentransfer
- Rollenbasiertes Rechtemanagement
- Segmentierung von Netzwerken
- Strukturierte Backupstrategie
- Virenschutzstrategie
- Monitoring der IT-Infrastruktur und regelmäßige Auswertung von Logfiles
- Vorhalten von Ersatzsystemen
- Softwareprodukte zur Sicherstellung der Datenintegrität
- Durchführung von Penetrationstests
- Anschaffung datenschutzkonformer Software
- Anpassung bestehender Software an die datenschutzrechtlichen Vorgaben

§

Geregelt wird die Pflicht zur Umsetzung der TOMs in Art. 32 DSGVO, § 26 KDG und § 27 DSG-EKD.

# Technisch-Organisatorische-Maßnahmen (TOMs): Organisatorische Aspekte

Neben den technischen Maßnahmen fordert der Datenschutz auch viele organisatorische Maßnahmen zum Schutz der Daten.
Beispiele hierfür sind:

- **Datenschutzrichtlinie**
  Festlegung, wie sich das Unternehmen und seine Mitarbeiter datenschutzkonform zu verhalten haben.
- **IT-Sicherheitsrichtlinie**
  Planung und Durchführungsanweisungen zur Entwicklung und Ausgestaltung der IT/TK-Infrastruktur.
- **Geheimhaltungsverpflichtung der Mitarbeiter**
  Alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind schriftlich auf das Datengeheimnis zu verpflichten.
- **Schulung und Sensibilisierung**
  Die Mitarbeiter müssen regelmäßig im Umgang mit personenbezogenen Daten und in der Anwendung der relevanten Datenschutzgesetzgebung geschult werden. Zudem sollten situationsbezogene Sensibilisierungen am Arbeitsplatz durch den Vorgesetzten stattfinden.
- **Schaffung eines datenschutzgerechten Arbeitsumfelds**
  Um datenschutzkonform arbeiten zu können, ist es erforderlich, den Arbeitsplatz der Mitarbeiter und das Arbeitsumfeld datenschutzgerecht zu gestalten.
- **Regelmäßige Kontrolle**
  Im Datenschutz wird eine regelmäßige Kontrolle der Einhaltung aller Vorgaben verlangt und sollte auch im eigenen Interesse durchgeführt und dokumentiert werden.
- **Einweisung der Führungskräfte**
  Da alle Führungskräfte für die Einhaltung des Datenschutzes in ihrem Bereich haften und dies sogar oftmals mit ihrem Privatvermögen, sollten sie regelmäßig mit ihren Pflichten vertraut gemacht werden.

§

Geregelt wird die Pflicht zur Umsetzung der TOMs in Art. 32 DSGVO, § 26 KDG und § 27 DSG-EKD.

# Auftragsverarbeitung

Oftmals kommt es vor, dass Daten nicht im eigenen Haus verarbeitet werden. Dies kann daran liegen, dass benötigtes Fachwissen nicht vorhanden ist, externe Softwarelösungen besser bzw. billiger oder die erforderlichen Kapazitäten nicht verfügbar sind. In all diesen Fällen gibt man Daten in die Hände Dritter. Dies ist jedoch auf Grund des Datengeheimnisses verboten, weshalb der Gesetzgeber Sonderfälle geschaffen hat, bei denen die Weitergabe trotzdem erlaubt ist. Einer hiervon ist die gemeinsame Verantwortlichkeit. Hierbei betreiben zwei oder mehr Verantwortliche eine gemeinsame Datenverarbeitung und haften auch beide vollumfänglich für alle Verstöße. Diese Lösung erfordert einen speziellen Vertrag, der die einzelnen Pflichten regelt und zuweist. Beispiele für eine solche gemeinsame Verantwortung sind facebook-Seiten, Arzneimittelstudien und Personalvermittlungsdienstleister.
Ein anderer Sonderfall ist die Auftragsverarbeitung. Hierbei gibt ein Auftraggeber seine Daten an einen Auftragnehmer, der sie gemäß den Anweisungen des Auftraggebers verarbeitet. Dazu muss ein spezieller Vertrag mit gesetzlich vorgegebenem Vertragsinhalt abgeschlossen werden. Der Auftraggeber muss den Auftragnehmer auf dessen Einhaltung sowie hinsichtlich der Umsetzung notwendiger Technisch-Organisatorischer-Maßnahmen regelmäßig kontrollieren. Zudem darf der Auftragnehmer ausschließlich gemäß der Anweisungen des Auftraggebers mit den Daten arbeiten. Die Haftung für die Einhaltung der Datenschutzgesetzgebung liegt bei beiden Parteien.

§

Geregelt wird die Auftragsverarbeitung in Art. 28 DSGVO, § 29 KDG und § 30 DSG-EKD. Die gemeinsame Verantwortung hingegen in Art. 26 DSGVO, § 28 KDG und § 29 DSG-EKD.

# Informationspflichten

Einer der wichtigsten Aspekte der DSGVO ist die Transparenz für den Betroffenen einer Datenverarbeitung. Hierzu hat der Gesetzgeber dem Verantwortlichen der Datenverarbeitung die Pflicht auferlegt, den Betroffenen unmittelbar bei Erhebung der Daten umfassend zu informieren. Liegen ihm diese Informationen bereits vor, muss nicht erneut informiert werden. Die Information muss mindestens folgende Inhalte enthalten:

- den Namen und die Kontaktdaten des Verantwortlichen
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf berechtigten Interessen beruht, die Darlegung und Erläuterung dieser Interessen
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer der Speicherung
- Erläuterung der verschiedenen Betroffenenrechte
- das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob eine Pflicht zur Bereitstellung (Angabe seiner Daten) besteht und die möglichen Folgen, die eine Nichtbereitstellung hätte
- Bei automatisierter Entscheidungsfindung (z.B. Kreditwürdigkeit), Bildung von Benutzerprofilen oder die Übermittlung ins außereuropäische Ausland müssen noch weitere Informationen enthalten sein.

# Rechtsgrundlagen

Generell ist die Verarbeitung personenbezogener Daten verboten, solange sich keine Rechtsgrundlage findet, die die Verarbeitung dieser Daten gestattet. Dies sind beispielsweise gesetzliche Pflichten, notwendige Daten zur Erfüllung eines Vertrags, die Einwilligung durch den Betroffenen oder das berechtigte Interesse des Unternehmens. Die beiden letztgenannten erfordern besondere Aufmerksamkeit.
Bei der Einwilligung sind mehrere Aspekte zu beachten und einzuhalten, da sonst die Einwilligung sofort ungültig und die Datenverarbeitung illegal wird.
Zuerst muss der Betroffene vollumfänglich über die geplante Verarbeitung seiner Daten aufgeklärt werden. Anschließend gibt er freiwillig ohne jeden Zwang und unmissverständlich seine Einwilligung. Diese Einwilligung darf jederzeit durch ihn widerrufen werden, ohne dass er negative Konsequenzen zu befürchten hat. Der Empfänger der Einwilligung hat diese rechtssicher nachweisbar zusammen mit dem Einwilligungstext für die gesamte Dauer der Datenverarbeitung zu speichern.
Ein weiterer Aspekt erschwert in neuester Zeit die Anwendung der Einwilligung. Die deutschen Aufsichtsbehörden gehen grundsätzlich davon aus, dass eine Einwilligung nach einem bestimmten Zeitraum automatisch ihre Gültigkeit verliert und erneuert werden muss. Leider sind diese Zeiträume derzeit in jedem Bundesland anders geregelt, längstens jedoch nach zwei Jahren.
Bei der Rechtsgrundlage des berechtigten Interesses ist zu beachten, dass eine schriftliche Abwägung der Interessen des Betroffenen an der Nicht-Verarbeitung seiner Daten und der Interessen des Verarbeiters an der Verarbeitung eben dieser durchgeführt und archiviert werden muss. Um diese Rechtsgrundlage anwenden zu dürfen, müssen bei der Abwägung die Interessen des Verarbeiters klar überwiegen.

§

Geregelt werden die Rechtsgrundlagen einer Datenverarbeitung in Art. 6 DSGVO, § 6 KDG und § 6 DSG-EKD.

GREAT OAK
DATENSCHUTZ

www.great-oak.de