


L c enh fter
Dat n chutz

Wir lösen Ihr Problem!



GREAT OAK II
DATENSCHUTZ



Datenmiss- brauch die mit? bieten mit fachmännischer Unterstützung

Was sich wo findet:

- 5 Über das Unternehmen Great Oak Datenschutz
- 6 Wer, wann, wie, wo?
- 8 Datenschutz an der Schnittstelle von Kirche und Staat
- 11 Der Auftrag lautet: Daten schützen!
- 12 Externe Experten – pro und contra
- 15 Was wir für Sie leisten – und was nicht
- 16 Dafür müssen Sie geradestehen
- 19 Teurer, als man denkt




Sehr geehrte Leserin, sehr geehrter Leser,

mit zunehmender Menge an verarbeiteten Daten wächst auch das Risiko eines Missbrauchs der vorhandenen Daten. Der Gesetzgeber hat das erkannt und versucht mit Gesetzen, wie der Datenschutzgrundverordnung (DSGVO), hier eine Struktur zu schaffen, sowie den Schutz der Betroffenen sicherzustellen. Einige Aspekte sind dabei gut gelungen, einige über das Ziel hinausgeschossen. Oftmals erscheint die DSGVO als Verursacher sinnlosen Bürokratieaufwands, was sich in vielen Fällen – bei eingehender Beschäftigung mit dem Thema – aber als gegenteilig herausstellt. Mein Unternehmen und ich unterstützen Sie bei der Umsetzung der aus den Gesetzen resultierenden Pflichten und Vorgaben, indem wir Ihnen maßgeschneiderte Lösungen bieten, bei denen Sie mit kleinstmöglichem Aufwand den gesetzlichen Anforderungen gerecht werden.

Ich freue mich auf eine zukünftige vertrauensvolle Zusammenarbeit mit Ihnen!

Florian Schirm
Geschäftsführer

A close-up photograph of a hedgehog in a natural, outdoor setting. The hedgehog is the central focus, with its spines clearly visible. It is surrounded by dry leaves and green foliage. A large, semi-transparent red circle is overlaid on the right side of the image, containing white text. The overall tone is somewhat muted, with a greenish-blue tint to the background.

Daten- tiefereis und Datenschutz

Kein Neuland für uns

Kerngeschäft statt Nebeneinkunft

Über das Unternehmen Great Oak Datenschutz

Seit 2007 sind wir als Datenschutzunternehmen in der gesamten Bundesrepublik tätig. Schon lange bevor überhaupt über die DSGVO gesprochen wurde, haben wir unsere Kunden mit angepassten und vor allem anwendbaren Datenschutzlösungen unterstützt. Wo erforderlich, haben wir zudem die Funktion des externen betrieblichen Datenschutzbeauftragten übernommen und so zur Erfüllung der gesetzlichen Vorgaben durch unsere Kunden beigetragen. Die Zufriedenheit unserer Kunden mit der Datenschutzberatung zeigt sich durch jahrelange Zusammenarbeit, teilweise schon seit der Gründung.

Wir betreuen dabei nicht nur größere Unternehmen und Kliniken, sondern kümmern uns besonders um die Datenverarbeiter, die keine eigene IT- und Rechtsabteilung besitzen und mit den vielen Datenschutzanforderungen zu kämpfen haben. Darunter sind Apotheken, Praxen, Kanzleien, Agenturen, KMU, Verbände sowie kirchliche Einrichtungen. Als reiner Datenschutzdienstleister bieten wir Ihnen ein umfassendes Know-How in den vielfältigen Bereichen des Datenschutzes. Bei uns ist Datenschutz nicht nur ein einträgliches Nebengeschäft, wir leben Datenschutz.

Wer, wann, wie, wo?

Über die Pflicht und Möglichkeit zur Bestellung eines Datenschutzbeauftragten

Angesichts der Komplexität und des Umfangs der Datenschutzpflichten ist die Bestellung eines Datenschutzbeauftragten die beste Maßnahme, die Sie ergreifen können. Auch wenn Sie keiner Pflicht zur Bestellung unterliegen, dürfen Sie jederzeit einen Datenschutzbeauftragten bestellen.

Einen Datenschutzbeauftragten zu haben, erleichtert Ihnen den Umgang mit dem Datenschutz ungemein. Nach außen zeigen Sie zudem, dass Sie das Thema ernst nehmen und die Daten der Kunden/Patienten bei Ihnen sehr gut aufgehoben sind. Letztendlich geben Sie auch ein Stück Haftung ab und können ruhiger schlafen.

Immer bestellen müssen Sie einen Datenschutzbeauftragten:

- **Wenn** Ihre Kerntätigkeit in der Verarbeitung besonders sensibler Daten (Art. 9 DSGVO) liegt (Schreibbüros, Archivierung, Apps im Gesundheitswesen usw.).
- **oder** Wenn Sie eine oder mehrere Datenverarbeitungen durchführen, die einer Datenschutzfolgenabschätzungspflicht unterliegen.
- **oder** Wenn in der Regel 20 oder mehr Personen bei Ihnen personenbezogene Daten digital verarbeiten. (Im kirchlichen Bereich bei 10 oder mehr Personen.)
- **oder** Wenn Sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.
- **oder** Ihre Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

§

Geregelt wird die Pflicht zur Bestellung eines Datenschutzbeauftragten in Art. 37 DSGVO, § 38 BDSG, § 36 KDG und § 36 DSG-EKD.

A young boy wearing a straw hat and a checkered shirt is sitting on the grass, leaning against the trunk of a large, old tree. He is holding an open book and appears to be reading. The scene is set in a park-like area with many trees and a grassy field. A large, semi-transparent red circle is overlaid on the image, containing white text.

Oft
vorgeschrieben
- immer sinnvoll



Datenschutz

an der Schnittstelle von Kirche und Staat

Zahlreiche unserer Kunden unterliegen der besonderen Gesetzgebung der Kirchen. Wir bieten Ihnen auch hier die notwendigen Fachkenntnisse, um in Ihrer Einrichtung den kirchlichen Datenschutz umzusetzen und laufend auf dem neuesten Stand zu halten. Unser Unternehmen vertritt die christlichen Werte und die Arbeit in kirchlichen und caritativen Einrich-

tungen stellt für uns einen wichtigen Aspekt unserer Datenschutzarbeit dar.

Durch die breit gefächerten Erfahrungen in den unterschiedlichen Datenschutzgesetzgebungen können wir Ihnen, neben der eigentlichen Umsetzung des kirchlichen Datenschutzes, auch bei allen Schnittstellen zur staatlichen Gesetzgebung Umset-



MeNsCHen- wÜRde und frEiHeiT

Christliche Werte,
die es zu schützen gilt

zungslösungen anbieten. Unsere Mitarbeiter kennen sich zudem mit den kirchlichen Besonderheiten, wie Verwaltungen und dem Aufbau der Kirchen aus. Eine weitere Besonderheit stellen kirchliche Einrichtungen dar, die eine Vielzahl weiterer staatlicher Gesetzgebungen zu beachten haben. Das betrifft Krankenhäuser, Pflegeheime, Kindergärten, aber auch kirchliche Verlage und Produktionswerkstätten. Hier

können Sie besonders von unserem Fachwissen aus beiden Gesetzgebungen profitieren und Datenschutzlösungen aus einer Hand bekommen.

Neben der Umsetzung des kirchlichen Datenschutzes bieten wir für Mitarbeiter der kirchlichen Einrichtungen spezielle Schulungen an, um sich mit der kirchlichen Gesetzgebung und deren Umsetzung vertraut zu machen.



Mit Leib
und Seele
für den Datenschutz

Der Auftrag lautet: Daten schützen!

Über die Aufgaben eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter hat die Aufgabe, auf die Einhaltung der gesetzlichen Vorgaben hinzuwirken. Er hat keine Befugnisse etwas zu bestimmen, ist aber im Umkehrschluss auch nicht für begangene Datenschutzverstöße des Unternehmens haftbar. Seine Tätigkeit besteht darin, Mitarbeiter in allen Datenschutzfragen zu beraten, die Geschäftsführung und Führungskräfte zur Einhaltung des Datenschutzes zu animieren, die Einhaltung der Schutzpflichten zu überwachen und als helfende Stelle für alle Betroffenen einer Datenverarbeitung zur Verfügung zu stehen. Hierzu hat der Datenschutzbeauftragte die Befugnis, alle personenbezogenen Daten im Unternehmen jederzeit einzusehen und zu prüfen. Zudem ist das Unternehmen verpflichtet, ihn

frühzeitig und ordnungsgemäß bei allen Datenverarbeitungen hinzuzuziehen.

Als externer Dienstleister kann der Datenschutzbeauftragte natürlich noch weitere Tätigkeiten übernehmen. So übernimmt er oftmals die umfangreichen regelmäßigen Auditierungs- und Kontrollpflichten der Führungskräfte, führt Schulungen durch und entwickelt datenschutzkonforme Lösungen für betriebliche Fragestellungen.

Im Rahmen seiner beratenden Tätigkeit übernimmt der externe Datenschutzbeauftragte natürlich die ganz normalen Haftungen des Dienstleisters. Bei internen Datenschutzbeauftragten ist diese jedoch auf die normale Arbeitnehmerhaftung begrenzt.

§

Geregelt werden die Tätigkeiten, Befugnisse und Aufgaben des Datenschutzbeauftragten in Art. 38 & 39 DSGVO, §§ 37 & 38 KDG und §§ 37 & 38 DSG-EKD.

Externe Experten – pro und contra

Über die Abwägung zwischen internen und externen Datenschutzbeauftragten

Falls Sie sich noch nicht entschieden haben, ob Sie einen Dienstleister beauftragen wollen oder doch einen eigenen Mitarbeiter zum betrieblichen Datenschutzbeauftragten bestellen wollen, haben wir Ihnen eine möglichst neutrale Tabelle zur Abwägung zur Verfügung zusammengetragen.

Externer Datenschutzbeauftragter

Vorteile

- Neutralität und fachliche Autorität gegenüber Mitarbeitern und Führungskräften
- Fest definierte Dienstleistung und Haftung im Rahmen des Vertrags
- Entfall eines Kündigungsschutzes
- Bessere Aus- und Fortbildung sowie hohes Transferwissen von anderen Mandaten
- Es müssen keine Räumlichkeiten und Ausstattung zur Verfügung gestellt werden

Nachteile

- Er ist nicht immer vor Ort, sondern nur zu vereinbarten Terminen
- In die betrieblichen Abläufe muss er sich erst einarbeiten
- Benötigt zusätzlich einen Datenschutzkoordinator vor Ort
- Auf Grund schlechter Kommunikation bekommt er vieles erst verspätet mit

Interner Datenschutzbeauftragter

Vorteile

- Kennt alle internen Abläufe
- Hat einen engen Kontakt zu den Mitarbeitern
- Ist ständig vor Ort
- Ab einer gewissen Größenordnung ist ein Mitarbeiter kostengünstiger als ein Dienstleister

Nachteile

- Er muss ausgebildet werden und jährlich zu Fortbildungen gehen
- Kündigungsschutz bis ein Jahr nach seiner Abberufung
- Ausstattung, Räumlichkeiten und ggf. weiteres Personal müssen ihm zur Verfügung gestellt werden
- Im Rahmen seiner Tätigkeit ist er weisungsfrei
- Fehlendes Transferwissen, da er nur die eigene Organisation kennt
- Autoritätsprobleme gegenüber Kollegen und Vorgesetzten
- Haftung nur in Höhe der normalen Arbeitnehmerhaftung

A young child with curly hair is peeking from behind a large, textured tree trunk in a forest. The child is wearing a blue and white striped shirt and blue jeans. The background is a blurred forest scene with green foliage and tree trunks. A large red circle is overlaid on the lower left side of the image, containing white text.

Ein Blick
von außen
öffnet die Augen



Etnlatsung
ni vieeln
Breeichen

- durch Unterstützung
von Great Oak

Was wir für Sie leisten – und was nicht

Über unsere Leistungen als betrieblicher Datenschutzbeauftragter

Wenn Sie sich für uns als betrieblicher Datenschutzbeauftragter entschieden haben, bekommen Sie einen unserer Mitarbeiter fest zugeteilt, der auch der Aufsichtsbehörde als Ihr Datenschutzbeauftragter gemeldet wird. Dieser Mitarbeiter betreut Sie im Tagesgeschäft und steht Ihnen als direkter Ansprechpartner zur Verfügung. Bei Abwesenheit wird er adäquat vertreten und bei schwierigen Sachverhalten zieht er optional weitere Kollegen mit hinzu, um Ihnen eine optimale Betreuung zu bieten.

Aufgaben, die wir für Sie übernehmen, sind:

- Auftritt nach außen als externer Datenschutzbeauftragter
- Feste Termine vor Ort
- Überwachung der Einhaltung datenschutzrechtlicher Pflichten
- Beratung der Führungskräfte im Umgang mit den Datenschutzgesetzen
- Information der Verantwortlichen über datenschutzbedeutsame Gesetze, Richtlinien und Rechtsprechung
- Grund- und Auffrischungsschulung der Mitarbeiter
- Durchführung von Audits zur Dokumentation des Datenschutzstands
- Erarbeitung von Verbesserungsvorschlägen
- Begleitung und Abnahme der Umsetzung von Verbesserungen
- Prüfung von Auftragsverarbeitungsverträgen
- Kommunikation mit den Aufsichtsbehörden

Allerdings bleiben trotz der Benennung eines betrieblichen Datenschutzbeauftragten auch noch Aufgaben und Tätigkeiten für Sie und Ihre Mitarbeiter übrig, da diese vom betrieblichen Datenschutzbeauftragten nicht übernommen werden können oder dürfen.

Diese sind beispielweise:

- Bestellung eines Koordinators vor Ort zur Unterstützung des Datenschutzbeauftragten
- Erfassung und Aktualisierung der Verfahren durch die jeweiligen Verantwortlichen
- Kontrolle der Mitarbeiter im Tagesgeschäft
- Unterstützung und Vorbereitung von Datenschutzaudits
- Anpassen und Einpflegen von durch den Datenschutzbeauftragten bereit gestellten Dokumenten
- Einhaltung der gesetzlichen Pflichten für Datenverarbeitungsverantwortliche

!

Falls Sie Ihren Datenschutz bisher noch nicht auf die Anforderungen der Datenschutzgrundverordnung angepasst haben oder das Thema Datenschutz neu angehen, sind einige grundlegende Maßnahmen umzusetzen, die nur einmalig anfallen. Hierzu bieten wir parallel zur Tätigkeit als Datenschutzbeauftragter ein gesondertes Projekt „Einführung Datenschutz“ an. Lesen Sie dazu auch unser „Handbuch zur Datenschutzeinführung“.

Dafür müssen Sie geradestehen

Über die Rechenschaftspflicht von Unternehmern in puncto Datenschutz

Das Grundprinzip der Datenschutzgrundverordnung lautet „Rechenschaftspflicht“ und gilt für alle, die personenbezogene Daten verarbeiten. Dieser Begriff meint, dass der Verantwortliche einer Datenverarbeitung jederzeit und umgehend nachweisen muss, dass er alle Pflichten der Datenschutzgrundverordnung erfüllt.

Die Missachtung dieser Pflichten führt zu empfindlichen Bußgeldern, insbesondere wenn sie aus Ignoranz der Thematik oder Vorsatz geschieht. Gleiches gilt für fehlende Nachweise. Neben dem Unternehmen haftet der Verantwortliche bei Missachtung sogar mit seinem Privatvermögen. Sie sollten deshalb das Thema sehr ernst nehmen und alle Nachweisdokumente unbedingt schriftlich und aktuell führen.

Diese sind u.a.:

- Für alle verarbeiteten Daten muss geprüft worden sein, ob diese rechtmäßig verarbeitet werden.
- Der Betroffene muss über die Verarbeitung informiert sein und sie lückenlos nachvollziehen können.
- Der Zweck der Verarbeitung muss eindeutig festgelegt und legitim sein.
- Der Umfang muss dem Zweck angemessen und so gering wie möglich gehalten werden.
- Die Richtigkeit der Daten muss gewährleistet sein.
- Für die gesamte Datenverarbeitung muss die Sicherheit der Daten, sowohl Vertraulichkeit als auch Integrität, gewährleistet sein.
- Die Daten dürfen nur zeitlich begrenzt für die Dauer des Zwecks gespeichert werden.
- Es muss gewährleistet sein, dass die Betroffenen ihre gesetzlich garantierten Rechte wahrnehmen können.

§

Geregelt wird die Rechenschaftspflicht in Art. 5, Abs. 2 DSGVO



iM dsCHunGel
der GeseTZli-
chEn VoRgaBEn

behalten wir
den Überblick



Am nächsten
Ende sparen
ist keine gute Idee

Teurer, als man denkt

Über Datenschutzverstöße und deren Bußgelder

Für Interessierte, die sich nicht dauerhaft mit dem Thema Datenschutz beschäftigen, ist es oftmals schwer, ein Gefühl dafür zu entwickeln, was richtig und falsch ist sowie welche Konsequenzen drohen können. Wir haben Ihnen beispielhaft einige Verstöße

und deren Konsequenzen zusammengetragen, damit Sie sich einen Überblick verschaffen können. Möchten Sie einen Blick auf aktuell geahndete Verstöße in der EU werfen, können Sie dies unter www.enforcementtracker.com tun.

Verstöße und deren Konsequenzen

Haga Hospital

- Unsicherer Umgang mit Patientendaten
- 460.000 Euro Bußgeld

Unbekanntes Unternehmen in Polen

- Verwendung öffentlicher Daten für Geschäftszwecke
- 219.538 Euro Bußgeld

Unbekanntes Unternehmen aus Deutschland

- Verspätete Meldung eines Datenschutzvergehens an die Aufsichtsbehörde und nicht korrekte Information der Betroffenen hierüber
- 20.000 Euro

IDdesign A/S

- Speicherung von personenbezogenen Daten über den Zweck hinaus
- 200.850 Euro Bußgeld

N26 (Bank)

- Führung einer schwarzen Liste mit ehemaligen Kunden
- 50.000 Euro Bußgeld

Privatperson

- Versenden einer E-Mail als Newsletter bei der alle Adressen der 153 Empfänger lesbar waren
- 2.000 Euro Bußgeld

Marriot International (Hotels)

- Verstoß gegen die Pflichten zur IT-Sicherheit aus Art. 32 DSGVO bei 339.000.000 Datensätzen
- 119.390.200 Euro Bußgeld

British Airways

- Verstoß gegen die Pflichten zur IT-Sicherheit aus Art. 32
- 204.600.000 Euro Bußgeld

Google

- Fehlerhafte Aufklärung der Benutzer über die Datenverarbeitung
- 50.000.000 Euro Bußgeld

§

Geregelt wird das Verhängen von Geldbußen in Art. 83 und Art. 84 DSGVO



GREAT OAK II
DATENSCHUTZ

www.great-oak.de