

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

Verpflichtungserklärung zur Einhaltung des Datengeheimnisses gemäß § 5 der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) sowie zur Wahrung der Schweigepflicht nach § 203 Strafgesetzbuch (StGB)

Klicken oder tippen Sie hier, um Text einzugeben.

(Name, Vorname)

Klicken oder tippen Sie hier, um Text einzugeben.

(Einsatzstelle / Funktion)

Ich verpflichte mich,

1. die Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG), sowie die anderen für mich und meine Tätigkeit geltenden Datenschutzregelungen, einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in der jeweils geltenden Fassung sorgfältig einzuhalten und alle personenbezogenen Angaben, die ich aufgrund meiner Tätigkeit erhalten habe oder die mir in diesem Zusammenhang zur Kenntnis gelangt sind, vertraulich zu behandeln,
2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten und
3. fremde Geheimnisse nur im notwendigen dienstlichen Zusammenhang zu gebrauchen. Damit sind zum persönlichen Lebensbereich gehörende Geheimnisse, wie auch Betriebs- und Geschäftsgeheimnisse, gemeint, die mir im Rahmen meiner beruflichen oder ehrenamtlichen Tätigkeit anvertraut wurden oder bekanntgeworden sind. Es kann nach § 203 Strafgesetzbuch strafbar sein, die oben genannten fremden Geheimnisse zu offenbaren. Diese strafrechtlich bewehrte Schweigepflicht gilt nach § 203 StGB insbesondere für Sozialpädagogen, Psychologen, Ärzte und Apotheker und das sie unterstützende Personal (beispielsweise Hospizmitarbeitende, Schwesternhelfer, Krankenschwestern, Rettungsassistenten und -sanitäter sowie Pflegekräfte).

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis disziplinarrechtliche bzw. arbeitsrechtliche / rechtliche Folgen haben kann. Gemäß § 203 StGB ist die unbefugte Offenbarung von fremden Geheimnissen strafbar und kann mit Geld- oder Freiheitsstrafe bestraft werden.

Eine Ausfertigung dieser Verpflichtungserklärung und ein Merkblatt zum Thema Datenschutz (inklusive der zu beachtenden Vorschriften) habe ich erhalten. Im Übrigen können die relevanten Vorschriften jederzeit in der Malteser DokBox¹ eingesehen werden.

Diese Erklärung wird zu den Akten genommen.

Ort, Datum, Unterschrift

Merkblatt Datenschutz

➤Datenschutz schützt das Persönlichkeitsrecht

Warum Datenschutz?

Ein wirksamer Datenschutz schützt das Persönlichkeitsrecht jedes Bürgers und will einer Beeinträchtigung des informationellen

¹ Mitgeltendes Dokument (KDR-OG - Gesetzestext), auffindbar in der DokBox.

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

Selbstbestimmungsrechts entgegenwirken. Dieses Recht soll dem Einzelnen ermöglichen, sich seine Privatsphäre zu erhalten und zu verhindern, dass er in zunehmender Abhängigkeit von Stellen in Staat, Wirtschaft und Verwaltung gerät, weil diese immer mehr von ihm wissen.

Zum Schutz des Persönlichkeitsrechts wurden daher verschiedene staatliche Rechtsvorschriften geschaffen, unter anderem auch das Bundesdatenschutzgesetz.

Aufgrund des durch das Grundgesetz bestimmten Rechts der katholischen Kirche, ihre Angelegenheiten selbst zu regeln und der in der Datenschutz-Grundverordnung enthaltenen entsprechenden Ermächtigung, wurde eine eigene Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) erlassen, die den besonderen kirchlichen Anliegen Rechnung trägt. Die KDR-OG kommt als spezialgesetzliche Regelung in den Malteser Unternehmen und Einrichtungen zur Anwendung.

Welche Daten werden geschützt?

➤ Geschützt werden personenbezogene Daten

Personenbezogene Daten sind alle Angaben zu einem Menschen, wie zum Beispiel Name und Anschrift, Telefonnummern, Vertragsbeziehungen, Angaben zu Vermögensverhältnissen. Zusammenfassend lässt sich also sagen, dass personenbezogene Daten alle Informationen sind, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei ist die technische Form der Angaben nicht von Bedeutung. Auch Fotos, Videoaufnahmen, Röntgenbilder oder Tonbandaufnahmen können personenbezogene Daten enthalten, sofern sie sich auf eine identifizierte oder identifizierbare Person beziehen. Um Angaben über eine identifizierte Person handelt es sich, wenn die Daten mit dem Namen der betroffenen Person verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Bezug unmittelbar

herstellen lässt. Identifizierbar ist eine Person, wenn ihre Identität mittels Zusatzwissen bzw. zusätzlichen Hilfsmitteln ohne unverhältnismäßigen Aufwand festgestellt werden kann.

Wann dürfen die personenbezogenen Daten verarbeitet werden?

➤ Nur wenn die KDR-OG oder eine andere Rechtsvorschrift die Verarbeitung erlaubt. Die Erlaubnis kann sich außerdem aus der Einwilligung des Betroffenen ergeben.

Es gilt das so genannte Verbotsprinzip. Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist verboten, solange diese nicht ausdrücklich durch eine Rechtsvorschrift erlaubt oder die Einwilligung vom Betroffenen eingeholt worden ist. In der KDR-OG und in anderen Rechtsvorschriften finden sich deshalb Regelungen, die eine Verarbeitung rechtfertigen und für zulässig erklären.

Im Rahmen der Einwilligungserklärung ist der Betroffene vorher umfassend über den Zweck und die weitere Verarbeitung zu informieren. Die Einwilligung muss zudem freiwillig erfolgen und eindeutig sein. Eine erteilte Einwilligung kann jederzeit widerrufen werden.

Welche Pflichten ergeben sich daraus für das Unternehmen?

➤ Das Unternehmen prüft im Einzelfall die Zulässigkeit der Verarbeitung und verpflichtet die betreffenden Mitarbeiter auf die Einhaltung des Datengeheimnisses.

Das Unternehmen hat daher zu prüfen, ob eine Rechtsgrundlage oder aber eine wirksame Einwilligung des Betroffenen im konkreten Einzelfall vorliegt.

Werden personenbezogene Daten ohne Kenntnis des Betroffenen erhoben, muss das

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

Unternehmen dem Betroffenen die erforderlichen Informationen gem. § 16 KDR-OG mitteilen, sofern der Betroffene nicht auf andere Art und Weise Kenntnis darüber erlangt. Das ist der Fall, wenn offensichtlich Daten verarbeitende Prozesse ein Vertragsverhältnis (Arbeitsvertrag, Kaufvertrag, Behandlungsvertrag) begleiten oder er selbst seine Daten zur Speicherung bekannt gibt (Bewerbung).

Sofern personenbezogene Daten unmittelbar beim Betroffenen erhoben werden, teilt das Unternehmen der betroffenen Person unmittelbar zum Zeitpunkt der Erhebung die gem. § 15 KDR-OG erforderlichen Informationen mit.

Welche Rechte hat ein Betroffener?

➤ Der Betroffene kann Auskunft, Berichtigung, Sperrung oder Löschung seiner Daten verlangen. Darüber hinaus steht der betroffenen Person ein Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und ein Widerspruchsrecht gegen bestimmte Verarbeitungsarten zu.

Die betroffene Person kann die zuständige Aufsichtsbehörde anrufen und Schadensersatz verlangen

Grundsätzlich kann der Betroffene jederzeit unentgeltlich Auskunft über alle zu seiner Person gespeicherten Daten verlangen.

Der Betroffene kann verlangen, dass falsche Daten berichtigt, unberechtigt gespeicherte oder unrichtige Daten gesperrt (der weiteren Verarbeitung entzogen) oder gelöscht werden. Die Sperrung von Daten ist vor allem dann angezeigt, wenn rechtliche Aufbewahrungsvorschriften einer sonst erforderlichen Löschung entgegenstehen.

Nicht zuletzt kann sich der Betroffene auch mit einer Beschwerde an die zuständige Aufsichtsbehörde wenden und wegen

unzulässiger oder falscher Datenverarbeitung Schadensersatz verlangen.

Wer kontrolliert den Datenschutz?

➤ Der Datenschutzbeauftragte des Unternehmens prüft den Datenschutz.

Der Datenschutzbeauftragte des Unternehmens prüft im Rahmen seiner Tätigkeit, ob die in Frage stehenden personenbezogenen Daten zulässig erhoben, zweckgebunden genutzt und unter angemessenen Sicherheitsvorkehrungen verarbeitet werden.

Er berät die Geschäftsleitung und steht bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten allen Mitarbeitern zur Verfügung.

Welche Konsequenzen können sich aus Datenschutzverletzungen ergeben?

➤ Es drohen Imageverlust, arbeitsrechtliche Konsequenzen, Bußgelder und Schadensersatzpflichten.

Unzulässige Veröffentlichungen von Kunden- und Mitarbeiterdaten führen in der Regel zu Imageschäden und in Folge zu erheblichen wirtschaftlichen Verlusten.

Werden die im Unternehmen getroffenen Datenschutz- und Datensicherheitsmaßnahmen grob fahrlässig oder vorsätzlich missachtet, können sich daraus arbeitsrechtliche Konsequenzen und Schadensersatzpflichten für den einzelnen Mitarbeiter ergeben.

Des Weiteren kann die zuständige Datenschutzaufsicht bei vorsätzlichen oder fahrlässigen Verstößen gegen Bestimmungen des KDR-OG Geldbußen verhängen. Schadensersatzpflichten entstehen, wenn Rechte der Betroffenen durch unzulässige Datenerhebung, Nutzung oder Verarbeitung verletzt werden.

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

Wie lange dürfen personenbezogene Daten aufbewahrt werden? Wie werden sie entsorgt?

➤ Die Aufbewahrung personenbezogener Daten ist nur so lange zulässig, bis der Zweck ihrer Speicherung erreicht wurde und daher ihre Kenntnis für die Erreichung des Zwecks nicht mehr erforderlich ist. Allerdings kann es passieren, dass diese eigentlich zu löschenden personenbezogenen Daten nicht gelöscht werden dürfen, weil etwa gesetzliche Regelungen eine Aufbewahrung vorschreiben. In einem solchen Fall tritt an die Stelle der Löschung die Sperrung der Daten.

Die nach gesetzlichen, satzungsgemäßen oder vertraglichen Vorschriften aufzubewahrenden Daten sind entsprechend ihrer Fristen und der notwendigen Sicherheitsstufe zu lagern.

Nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen sind zu vernichtende Datenträger (Papier, Disketten, Datenbänder, CD-ROM usw.) entweder mittels Aktenvernichter zu vernichten oder einem Unternehmen zu übergeben, das als zuverlässiger und zertifizierter Auftragsverarbeiter für die Datenentsorgung gilt. Keinesfalls dürfen personenbezogene (oder auch sonstige sensible firmeninterne) Daten dem allgemeinen Haus- oder Papiermüll zugeführt werden.

Ein einfaches Löschen von Dateien auf dem PC ist in der Regel nicht ausreichend, da die Daten mit einfachen Mitteln wieder lesbar gemacht werden können. Wenden Sie sich im Bedarfsfall für eine datenschutzkonforme Löschung von Dateien an ihren IT- Verantwortlichen oder an das User Help Desk der SoCura GmbH.

Was versteht man unter Datensicherheit?

➤ Unter Datensicherheit wird der Schutz von Daten vor Verlust, Verfälschung, Beschädigung oder Löschung durch organisatorische und technische Maßnahmen und durch Software verstanden.

Jede verantwortliche Stelle hat die bei ihr gespeicherten Daten vor Verlust, Verfälschung, Beschädigung oder Löschung gesichert aufzubewahren. Das erfordert von den Mitarbeitern eine erhöhte Aufmerksamkeit beim Transport von Daten, beim Umgang mit dem Passwort, dem Verschluss der Unterlagen gegen unberechtigte Einsicht und bei der Kontrolle von Dienstleistern (z.B. Reinigungsunternehmen, Datenentsorgung, IT - Wartung).

Haben Sie noch Fragen?

Sie sind sich nicht sicher, ob eine Datenerhebung, Verarbeitung oder Nutzung rechtmäßig erfolgt?

Sie haben Fragen, Anregungen oder Kritik zu Datenschutzthemen?

Kontaktieren Sie den für Sie zuständigen Datenschutzkoordinator.

Falls Ihnen der für Sie zuständige Datenschutzkoordinator nicht bekannt ist, können Sie diesen im Dokument Datenschutzkoordinatoren im Malteser Verbund – Übersicht² finden.

² Mitgeltendes Dokument (Datenschutzkoordinatoren im Malteser Verbund-Übersicht), auffindbar in der DokBox.

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

Gesetzliche Vorschriften:

Auszug aus der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG)

§ 5 (Datengeheimnis)

Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Auszug aus dem Strafgesetzbuch (StGB)

§ 203 StGB (Verletzung von Privatgeheimnissen)

- Auszug -

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. ...
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.

5. ...

6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7. ...

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

Datengeheimnis Verpflichtung und Wahrung der Schweigepflicht

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Mitgeltende Unterlagen

→ [DSK Datenschutzkoordinatoren im Malteser Verbund - Übersicht](#)