

Verpflichtung auf das Datengeheimnis und Verschwiegenheitspflicht

Angaben zum zu Verpflichtenden

Name, Vorname: _____

Personalnummer: _____ Telefon: _____

Abteilung/Betrieb: _____

wird wie folgt auf das Datengeheimnis verpflichtet und auf die Strafbarkeit von Verstößen hingewiesen:

Es ist Ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten.

Verstöße gegen das Datengeheimnis können nach Art. 83 DS-GVO i. V. m. §§ 41-43 BDSG mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden.

Darüber hinaus werden Sie auf die in Ihrem Arbeitsvertrag und der Arbeitsordnung enthaltene Verschwiegenheitspflicht hingewiesen, die durch die Verpflichtung auf das Datengeheimnis nicht berührt wird.

Diese Verpflichtung wird an die Personalabteilung weitergegeben und ist Bestandteil der Personalakte.

Die Verpflichtungen bestehen auch nach Beendigung des Beschäftigungsverhältnisses fort.

Das Merkblatt als Anlage zu dieser Erklärung habe ich erhalten.

Mit Ihrer Unterschrift bestätigen Sie diese Verpflichtung sowie den Inhalt der vorstehenden Belehrung und des Merkblatts verstanden zu haben.

Datum, Unterschrift Mitarbeiter/in

Merkblatt

Verpflichtung auf das Datengeheimnis

1. Gesetzliche Grundlagen

Neben den betrieblichen Geheimhaltungsvorschriften gelten für Sie aufgrund Ihrer Aufgabenstellung die Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Wir verpflichten Sie, das Datengeheimnis zu wahren. Hiernach ist es Ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese Verpflichtung ist Teil des Arbeitsvertrages und erlischt nicht, wenn Sie eine andere Aufgabe im Konzern übernehmen oder das Unternehmen verlassen.

Verstöße gegen das Datengeheimnis können nach Art. 83 DS-GVO i. V. m. §§ 41-43 BDSG mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben.

Sofern Sie in folgenden Bereichen tätig sind gelten für Sie zusätzlich folgende Regelungen:

Wenn Sie im IT-Bereich tätig sind kann es zudem dazu kommen, dass Sie mit Telekommunikationsdaten in Berührung kommen. Diese Daten können ggf. dem Fernmeldegeheimnis unterliegen (§ 88 TKG). Eine Verletzung des Fernmeldegeheimnisses ist zum einen strafbar (§ 206 StGB), die Verletzung von Telekommunikationsschutzvorschriften (§ 91 ff. TKG) zum anderen aber auch bußgeldbewehrt (§ 149 TKG).

Durch die Arbeit in unserem Hause können Sie im Rahmen Ihrer Arbeitsaufgabe auch Zugriff auf Patientendaten haben. Sie werden daher auch über Ihre Pflicht zur Wahrung des Patientengeheimnisses (Ärztliche Schweigepflicht) nach § 203 Strafgesetzbuch in Kenntnis gesetzt. Sie werden zudem darauf hingewiesen, dass eine Offenbarung von Patientengeheimnissen ohne Einwilligung des Patienten auch gegenüber anderen Mitarbeitern nur erlaubt ist, wenn diese an der Betreuung, Behandlung oder deren Dokumentation und Abrechnung beteiligt sind.

2. Erläuterung der wichtigsten gesetzlichen Bestimmungen

2.1 Aufgabe des Datenschutzes

Aufgabe des Datenschutzes ist es, Persönlichkeitsrechte des Menschen zu schützen: Seine individuellen Daten dürfen bei ganz oder teilweise automatisierter Verarbeitung sowie bei nichtautomatisierter Verarbeitung und Speicherung in einem Dateisystem nicht zweckentfremdet oder missbraucht werden. Im Rahmen eines Beschäftigungsverhältnisses gelten die gesetzlichen Regelungen zum Datenschutz auch für sonstige Unterlagen, die weder (teil-)automatisiert verarbeitet

noch in einem Dateisystem gespeichert werden.

2.2 Personenbezogene Daten

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Beispiele: Name, Anschrift, Geburtsdatum, Ausbildung, Gesundheitszustand, Kauf- und Zahlungsgewohnheiten, familiäre und finanzielle Verhältnisse von Mitarbeitern, Bewerbern, Kunden, Interessenten, Lieferanten, Fremdkräften.

2.3. Verarbeitung

„Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

2.4. Zulässigkeitsvoraussetzungen

Eine Erlaubnis zum Verarbeiten personenbezogener Daten zur Erfüllung von Geschäftszwecken des Unternehmens besteht nur,

- wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der das Unternehmen unterliegt, z. B. aufgrund von Steuer- und Sozialgesetzen, HGB, AktG, BetrVG, Tarifverträgen, Gerichtsbeschluss;
- wenn die betroffene Person vorab wirksam eingewilligt hat (in der Regel schriftlich);
- wenn dies für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist oder zur Durchführung einer vorvertraglichen Maßnahme, die auf Anfrage der betroffenen Person erfolgt, erforderlich ist (z. B. Arbeits-, Kauf-, Mietvertrag);
- soweit es zur Wahrung berechtigter Interessen der speichernden Stelle oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Interessenabwägung);
- wenn dies erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Personenbezogene Daten dürfen darüber hinaus nur in Einklang mit Weisungen des Verantwortlichen verarbeitet werden. Neben Einzelweisungen der Vorgesetzten gelten als Weisung:

Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen, Richtlinien sowie betriebliche Dokumentationen und Handbücher

2.5. Grundsätze für die Verarbeitung, insbesondere Zweckbindung

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden („Zweckbindung“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“); Daten sind daher in der Regel nach dem Wegfall des Zwecks der Speicherung zu löschen. Hierbei sind gesetzliche und interne Aufbewahrungsfristen zu beachten.
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“). Beachten Sie hierzu bitte die internen Regelungen, insbesondere solche zur Informationssicherheit, die Sie im Intranet in der Rubrik Datenschutz abrufen können.

2.6. Informationspflicht

Sie müssen den Datenschutzbeauftragten über geplante Systeme und Datenverarbeitungen mit personenbezogenen Daten rechtzeitig informieren.

2.7. Anfragen externer Stellen

Bei einzelnen, im öffentlichen Interesse stehenden Ausnahmetatbeständen ist eine Datenweitergabe zusätzlich erlaubt (z. B. Erteilung von Auskünften an die Polizei bei Vorliegen einer staatsanwaltlichen Verfügung oder eines richterlichen Beschlusses, Flucht- oder Verdunkelungsgefahr). Anfragen von Banken, Versicherungen, Rechtsanwälten usw. dürfen sofern sie nicht von einer in Punkt 2.4. aufgeführten Zulässigkeitsvoraussetzungen gedeckt sind - grundsätzlich nicht ohne Einwilligung der betroffenen Person beantwortet werden. In Zweifelsfällen sollte vor einer Datenübermittlung der Datenschutzbeauftragte eingeschaltet werden.

2.8. Datensicherung

Die personenbezogenen Daten sind in einer Weise zu verarbeiten, die ihre angemessene Sicherheit gewährleistet. Davon umfasst sind geeignete technische und organisatorische Maßnahmen zum

Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

3. Datenschutz als permanente Aufgabe

Es liegt in Ihrem und in unserem Interesse, sowohl die gesetzlichen Verpflichtungen nach den geltenden Datenschutzbestimmungen (insbesondere DSGVO und BDSG) als auch die betrieblichen Geheimhaltungsvorschriften strikt einzuhalten.

Mitarbeiter, denen bei der Datenverarbeitung oder in sonstiger Weise **personenbezogene Daten** zur Kenntnis gelangen, dürfen diese nur im Rahmen ihrer Aufgabenerfüllung verwenden und haben sie gegenüber Unbefugten geheim zu halten.

Sanofi wird Ihnen zum Datenschutz Informationen, Schulungen und weitere Möglichkeiten zur Verfügung stellen.

Sollten Sie Mängel hinsichtlich Datenschutz, Datensicherung und Ordnungsmäßigkeit der Datenverarbeitung feststellen, werden Auskünfte über personenbezogene Daten von Ihnen gefordert oder haben Sie Fragen zum Thema Datenschutz, so wenden Sie sich bitte an Ihre Führungskraft oder an das data privacy team. Bei vertraulichen Anfragen können Sie sich auch direkt an den Datenschutzbeauftragten wenden. Die Kontaktdaten finden Sie im Intranet in der Rubrik Datenschutz.

4. Gesetzliche und betriebliche Regelungen

Auszüge aus den gesetzlich und betrieblichen Regelungen den Datenschutz betreffend können Sie im Intranet unter der Rubrik Datenschutz einsehen.