afm | unternehmensgruppe assekuranz-finanz-makler

Datenschutz

afm Richtlinie

Stand 05-2018

Liebe Kolleginnen und Kollegen,

der Datenschutz hat in den letzten Jahren aufgrund der weitgehenden elektronischen Abwicklung sowie zunehmender gesetzlicher Regelungen einen immer höheren Stellenwert erreicht.

afm nimmt den Datenschutz beim Umgang mit den Daten der Interessenten und Kunden sehr ernst und will den rechtlichen Anforderungen an die Erhebung und Verarbeitung personenbezogener Daten gerecht werden.

Ein gewissenhafter Umgang mit diesen Daten wird von unseren Kunden und Geschäftspartnern vorausgesetzt und bildet somit die Grundlage für eine vertrauensvolle Geschäftsbeziehung.

Diese Datenschutzrichtlinie benennt die Regularien für den Umgang mit persönlichen Daten.

Die Umsetzung der aus den Datenschutzrichtlinien folgenden Verpflichtungen und die Einhaltung der DSGVO sowie die der nationalen Datenschutzgesetze werden durch die Führungskräfte und Mitarbeiter im Unternehmen sichergestellt.

Die Geschäftsleitung

Inhalt

1. Ziel der Datenschutzrichtlinie

Die Daten der Kunden und Partner sind ein wichtiger Wettbewerbsfaktor und tragen in großem Umfang zur Wertschöpfung der afm Gruppe bei. Diese Daten sind gegen Gefährdungen eines unzulässigen Zugriffs zu schützen. Neben diesem technischen Schutz erwarten die Kunden und Partner aber auch generell einen sorgsamen Umgang mit ihren Daten. Ohne eine vertrauensvolle Beziehung zu den Kunden und Partnern sind dauerhafte Geschäftsbeziehungen nicht realisierbar.

afm bekennt sich zu seiner Verantwortung im Umgang mit den Daten und gibt sich mit dieser Richtlinie einen einheitlichen Datensicherheitsstandard für die Verarbeitung personenbezogener Daten von Kunden und Partnern. Die Richtlinie unterstützt die Wettbewerbsfähigkeit des Konzerns und stellt eine Basis für eine dauerhafte und vertrauensvolle Geschäftsbeziehung dar. So ist gewährleistet, dass das von der Europäischen Datenschutzrichtlinie (DSGVO) und den nationalen Gesetzen (bspw. BDSG n.F.) ausgehende und verlangte Schutzniveau gewahrt bleibt.

2. Geltungsbereich, -dauer und Änderung der Richtlinie

Diese Richtlinie gilt für alle Unternehmen der afm Gruppe und deren Mitarbeiter und erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten von Kunden, Interessenten und Partnern.

Anders als nicht-anonymisierte Daten unterliegen die anonymisierten Daten bspw. für statistische Auswertungen oder Untersuchungen, nicht dieser Datenschutzrichtlinie.

Eine Änderung dieser Richtlinie findet ausschließlich durch den Beauftragten für den Datenschutz statt.

Die Gesellschaften haben die Bestimmungen dieser Richtlinie in der jeweils gültigen Fassung zu befolgen. Nur für den Fall, dass damit eine Verschlechterung der Position des Betroffenen verbunden sein sollte, gilt diejenige Fassung, die zum Zeitpunkt der Verarbeitung seiner Daten galt.

Die Richtlinie tritt mit dem 25.05.2018 in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird. Die jeweils neueste Version der Datenschutzrichtlinie kann im BeraterPortal eingesehen werden.

3. Geltung staatlichen Rechts

Die vorliegende Datenschutzrichtlinie ist ergänzend zum geltenden nationalen Datenschutzrecht zu lesen und deckt auch die Datenschutzprinzipien der Europäischen Union umfassend ab. Dabei geht das nationale Recht (bspw. BDSG n.F.), nur dann der Datenschutzgrundverordnung mit ihrer unmittelbaren Wirkung vor, wenn ein Aspekt durch die Verordnung nur rudimentär umschrieben und der Konkretisierung bedarf. Hat entgegen aller Erwartung der nationale Gesetzgeber keine dieser Datenschutzrichtlinie entsprechende Regelung vorgesehen, so setzt diese Datenschutzrichtlinie gleichwohl verbindliches Recht für den Verantwortlichen.

Im Übrigen werden die Meldepflichten für eine etwaige Datenverarbeitung stets beachtet.

Im Falle eines Widerspruches zwischen den gesetzlichen Regelungen der Bundesrepublik Deutschland zum Datenschutz und dieser Datenschutzrichtlinie, wird der Datenschutzbeauftragte nach einer gesetzeskonformen Lösung im Sinne dieser Datenschutzrichtlinie suchen.

4. Grundsätze für die Verarbeitung personenbezogener Daten

a) Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Daten müssen fair und auf rechtmäßige Weise verarbeitet werden.

b) Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich. Diese können aufgrund vertraglicher Vereinbarungen mit dem Betroffenen, einer Einwilligung des Betroffenen oder aufgrund staatlichen Rechts stattfinden.

c) Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben.

Bei Erhebung der Daten muss der Betroffene folgendes erkennen können oder entsprechend informiert werden über:

- Die Identität der verantwortlichen Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Der Betroffene sollte über die Freiwilligkeit der Angabe von Daten für Zwecke des Marketings unterrichtet werden.

In Konzernstandards werden Vorgaben zu erforderlichen Informationen über den Umgang mit den Daten des Betroffenen gemacht.

Neben den Vorgaben in Konzernstandards können aufgrund staatlichen Rechts zusätzliche oder abweichende Anforderungen an den Inhalt und Umfang der Informationen bestehen. Dies können zum Beispiel Vorgaben zu Informationen über ein Widerspruchsrecht des Betroffenen gegen Kontakte zu Marketing- und Werbezwecken sein.

d) Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden ob und in welchem Umfang diese notwendig ist, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter Daten erfolgen, sind nicht von dieser Richtlinie erfasst.

Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben.

Daten, die nicht mehr benötigt werden, sollen unter Beachtung bestehender Aufbewahrungspflichten gelöscht werden.

e) Sachliche Richtigkeit, Datenaktualität

Personenbezogene Daten sind richtig und auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende oder unvollständige Daten gelöscht, berichtigt oder ergänzt werden.

f) Besonders schutzbedürftige Daten

Besonders schutzbedürftige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein; oder die Verarbeitung ist notwendig, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Der Betroffene kann auch ausdrücklich in die Verarbeitung einwilligen.

g) Need-To-Know Prinzip

Vor dem Hintergrund der immer flexibleren Arbeitsorganisation ist darauf zu achten, dass Mitarbeiter Zugang zu personenbezogenen Daten nur nach dem Need-To-Know Prinzip erhalten. Das Need-To-Know Prinzip bedeutet, dass Mitarbeiter nur nach Art und Umfang ihrer jeweiligen Aufgaben Zugang zu personenbezogenen Daten erhalten dürfen. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten und deren Umsetzung.

h) Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, müssen besondere Voraussetzungen erfüllen. Sie dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden. Dem Betroffenen muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden. Strengere Vorgaben aufgrund staatlichen Rechts für automatisierte Einzelentscheidungen sind zu beachten.

i) Löschung

Nach dem Ablauf der geschäftsbedingten bzw. gesetzlichen Aufbewahrungsfristen, müssen personenbezogene Daten, die nicht mehr erforderlich[1] sind, gelöscht werden.

Abweichend davon, müssen Daten, die ein schutzwürdiges Interesse (bspw. nach HGB) oder historische Bedeutung(Unternehmensarchiv) genießen, weiterhin gespeichert bleiben, bis das schutzwürdige Interesse bzw. die historische Bedeutung rechtlich abschließend geklärt worden ist.

[1] vgl. Definition unter Anhang

5. Zulässigkeit der Datenverarbeitung

I. Kundendaten

a) Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des Betroffenen dürfen zur Durchführung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners nach Abschluss des Vertrages, sofern dies im Zusammenhang mit dem Vertragszweck steht. Kundenbindungs- oder Werbemaßnahmen sind davon nicht umfasst.

In der Vertragsanbahnungsphase ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Anträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüber hinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter 5 b) beachtet werden.

b) Datenverarbeitung zu Werbezwecken

Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. In der Regel trifft dies bei vorliegendem Maklerauftrag (Gesamtmandat) zu und umfasst auch den Versand von Medien wie zum Beispiel dem „Marktplatz“ und den Update Newsletter. In anderen Fällen, insbesondere im allgemeinen Neukundenanalyseverfahren sowie bei anlassbezogenen Beratungen, sollte im Rahmen der Kommunikation mit dem Betroffenen eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. (s. 5 c)).

Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen der afm Gruppe (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens unabhängig von dem Vorliegen einer Einwilligung immer zulässig.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig.

c) Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Insbesondere im allgemeinen Neukundenanalyseverfahren sowie bei anlassbezogenen Beratungen (auch Belegschaftsgeschäft außerhalb echter Gruppenverträge, wie beispielsweise Verträge der bAV) ist diese Einwilligung einzuholen. Vor der Einwilligung muss der Betroffene gemäß Punkt 4 c) dieser Datenschutzrichtlinie informiert werden, was mit unserer Einwilligungserklärung (Formular „Allgemeine Information und Einwilligung zur Datenverarbeitung“) erfüllt wird.

Die Einwilligungserklärung ist aus Beweisgründen regelmäßig schriftlich oder elektronisch einzuholen und zu dokumentieren. Die Dokumentation hat über das Kundenverwaltungsprogramm zu erfolgen (Ablage der gegengezeichneten Erklärungen im Reiter „Dokumente“). Zusätzlich ist eine Kennzeichnung über den Reiter „Merkmale“ innerhalb der Merkmalsübersicht erforderlich und vorzunehmen.

Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Dokumentation sowie die Kennzeichnung, sind in diesem Fall ebenfalls über das Kundenverwaltungsprogramm vorzunehmen und ggf. im weiteren Beratungsverlauf schriftlich nachzuholen.

Besondere Anforderungen an die Einwilligungserklärung aufgrund staatlichen Rechts sind einzuhalten.

d) Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

e) Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der verantwortlichen Stelle oder einer dritten Stelle erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftlich (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Diese sind für jede Verarbeitung zu prüfen.

f) Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen verarbeitet werden, soweit der Betroffene ausdrücklich seine darauf bezogene Einwilligung erklärt hat oder das Gesetz die Verarbeitung als erforderlich festschreibt. Eine zwingende Notwendigkeit der Datenverarbeitung begründet deren Zulässigkeit und ist gegeben, wenn dadurch rechtliche Ansprüche gegenüber dem Betroffenen geltend gemacht, ausgeübt oder verteidigt werden können.

Zeichnet sich die alsbaldige Datenverarbeitung besonders schutzwürdiger Interessen ab, so ist der Datenschutzbeauftragte des Verantwortlichen vor der tatsächlichen Verarbeitung zu informieren.

g) Automatisierte Einzelentscheidungen

Der Fortschritt ermöglicht technisch sogenannte automatisierte Einzelentscheidungen. Gleichwohl dürfen diese nicht die ausschließliche Grundlage für Entscheidungen mit abschlägigen rechtlichen Folgen oder gar erheblichen Beeinträchtigungen für den Betroffenen sein. Das diesem automatisierten Entscheidungsprozess entspringende Ergebnis ist neben der Information über den Einsatz der automatisierten Form, dem Betroffenen zusammen mit einer Möglichkeit zur Stellungnahme mitzuteilen. Das Risiko einer automatisierten Fehlentscheidung muss durch eine Plausibilitätsprüfung eines Mitarbeiters minimiert bzw. annähernd ausgeschlossen werden.

h) Nutzerdaten und Internet

Die Betroffenen sind über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf den Webseiten und Apps des Verantwortlichen in den Datenschutz- und Cookie-Hinweisen zu informieren. Dabei sind die Datenschutz- und Cookie-Hinweise leicht erkennbar, unmittelbar erreichbar und dauerhaft verfügbar für den Betroffenen zu implementieren.

Der Verantwortliche informiert den potentiell Betroffenen in den Datenschutzhinweisen auch über eine etwaige Auswertung oder Anfertigung eines Nutzungsprofils über das Nutzungsverhalten von Webseiten- und App-Benutzern (bspw. Klickzahlen bei Newslettern, frei zugänglichen Webinaren oder Downloadzahlen der online bereitgestellten Muster-Maklerverträge).

Ein solches Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder aber der Betroffene seine Einwilligung gegeben hat.

Wird das Tracking unter Verwendung eines Pseudonyms durchgeführt, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden.

II. Mitarbeiterdaten

a) Datenverarbeitung das (sich anbahnende) Arbeitsverhältnis betreffend

Die Begründung, die Durchführung oder die Beendigung des Arbeits-, Anstellungs- oder Dienstverhältnisses kann eine Verarbeitung personenbezogener Daten erforderlich machen. Ist dies der Fall, so darf sie erfolgen, insbesondere bei der Anbahnung eines Arbeitsverhältnisses ist eine Verarbeitung von erhaltenen personenbezogenen (Bewerber-)Daten erlaubt. Die erhaltenen (Bewerber-)Daten sind unter Berücksichtigung beweisrechtlicher Fristen nach einer erteilten Ablehnung zu löschen. Dies gilt nicht, wenn der Bewerber in eine erneute Verwendung seiner Daten zu einem späteren Zeitpunkt im Rahmen eines erneuten Auswahlverfahrens gegebenenfalls auch innerhalb der verantwortlichen Stelle eingewilligt hat.

Ist der Auswahlprozess ausgegliedert und wird mit Hilfe externer Dritte durchgeführt, so stellt die Verantwortliche Stelle vertraglich sicher, dass mit Mitarbeiterdaten DS-GVO compliant umgegangen wird.

Eine Einwilligung hat stets auch dann zu erfolgen, wenn die (Bewerber-)Daten aus dem ursprünglichen Bewerbungsprozess in einem späteren erneuten Auswahlverfahren bezüglich gleicher oder eine andere Position betreffend gewünscht ist.

Die Verarbeitung der (Bewerber-)Daten hat sich stets am Zweck des Arbeitsvertrages zu orientieren und darf nur in den nachfolgend abschließend aufgezählten Ausnahmefällen davon abweichen:
Bei einer erforderlichen Erhebung weiterer Informationen über den Bewerber bei Dritten, während der Anbahnungsphase des Arbeitsverhältnisses, hat sich diese an den gesetzlichen Regelungen der Bundesrepublik Deutschland zu orientieren. Bei verbleibenden Zweifeln der Verantwortlichen Stelle ist zur Wahrung der Rechtmäßigkeit der Erhebung eine Einwilligung bezogen auf die weiteren Informationen nötig.

Werden personenbezogene Daten nicht explizit für die Durchführung des Arbeitsverhältnisses verarbeitet, ist jeweils eine rechtliche Grundlage von Nöten. Diese kann sich aus dem Gesetz, einer ggf. kollektiven Regelung (Betriebsvereinbarung, Tarifvertrag), dem berechtigten nachzuweisenden Interesse der Verantwortliche Stelle oder der gesonderten Einwilligung des Mitarbeiters ergeben.

b) Datenverarbeitung aufgrund gesetzlicher oder kollektivrechtlicher Erlaubnis

Eine Datenverarbeitung ist immer dann zulässig, wenn diese aufgrund staatlicher Vorschriften verlangt, vorausgesetzt oder aber gestattet ist. Dabei müssen die Art und der Umfang der gesetzlich zulässigen Verarbeitung auch erforderlich sein und sich nach den staatlichen Vorschriften richten. Räumen diese einen sogenannten Handlungsspielraum ein, sind die schutzwürdigen Interessen des betroffenen Mitarbeiters hinreichend zu beachten.

Grundsätzlich findet die Datenverarbeitung zum Zwecke der Vertragsabwicklung statt. Eine über diesen Zweck hinausgehende Verarbeitung ist ebenfalls zulässig, wenn sie durch kollektivrechtliche Vorschriften (also Regelungen) erlaubt ist. Diese kollektivrechtlichen Regelungen (etwa ein Tarifvertrag) müssen jedoch den konkreten Verarbeitungszweck regeln.

c) Einwilligung in die Datenverarbeitung

Eine weitere Möglichkeit der Datenverarbeitung bildet die Einwilligung des Betroffenen Mitarbeiters. Diese Einwilligung ist nur freiwillig zu erklären. Jede Erklärung die deren Unfreiwilligkeit vermuten lässt, führt zur Unwirksamkeit der Einwilligungserklärung.

Schon aus beweisrechtlichen Gründen ist die Einwilligung schriftlich (iSv. § 126 BGB) einzuholen. Sie kann jedoch auch in elektronischer Form (iSv. 126 a BGB) erfolgen. Nur wenn im Einzelfall beide Varianten nicht durchführbar sind, wäre eine mündliche Einwilligung denkbar. Gleichwohl besteht auch in einem solchen Fall eine Pflicht zur ordnungsgemäßen Dokumentation. Schreiben nationale Vorschriften keine Einwilligung vor und gibt der Betroffene seine Daten freiwillig an, ist eine Einwilligung anzunehmen. Der Betroffene ist vor der Einwilligung gemäß 4 c) Datenschutzrichtlinie transparent zu informieren.

d) Datenverarbeitung aufgrund berechtigten Interesses

Besteht für die Verantwortliche Stelle ein berechtigtes Interesse, so kann eine Verarbeitung personenbezogener Daten ebenfalls erfolgen. Unter einem berechtigten Interesse versteht man rechtlich oder wirtschaftlich tragende Gründe.

Zu den rechtlichen Gründen zählen insbesondere die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, zu den wirtschaftlichen beispielsweise die Bewertung des Unternehmens.

Ergeben sich im Einzelfall Indizien für ein schutzwürdigeres Interesse eines Mitarbeiters, so darf trotz des berechtigten Interesses der Verantwortlichen Stelle eine Verarbeitung personenbezogener Daten nicht erfolgen. Dabei ist die Feststellung des schutzwürdigeren Interesses je Verarbeitungsvorgang vorzunehmen.

Die Verarbeitung von Mitarbeiterdaten im Rahmen von Kontrollmaßnahmen darf nur bei einer gesetzlichen Verpflichtung oder einem begründeten Anlass dazu erfolgen. Bei letzterem ist gleichwohl eine Verhältnismäßigkeitsprüfung der Kontrollmaßnahme durchzuführen. Dabei müssen die berechtigten Interessen des Unternehmens an der Kontrollmaßnahme (bspw. unternehmensinterne Regelungen, rechtliche Vorgaben) gegen die schutzwürdigen Interessen des Mitarbeiters am Ausschluss der Maßnahme in Abwägung gebracht werden. Nur wenn diese Abwägung zu einem Überwiegen der berechtigten Interessen des Unternehmens führt, ist die Verarbeitung der Mitarbeiterdaten angemessen (steht also im richtigen Verhältnis). Deshalb sind bereits vor jeder Maßnahme die Interessen beider Seiten zu dokumentieren. Auch sind eventuell bestehende Mitbestimmungs- und Informationsrechte (weitergehende Rechte) der Betroffenen zu berücksichtigen.

e) Verarbeitung besonders schutzwürdiger Daten

Eine Verarbeitung besonders schutzwürdiger Daten darf nur unter ganz bestimmten Voraussetzungen erfolgen. Besonders schutzwürdige Daten sind definiert als Daten über Gesundheit und Sexualleben, politische Meinung, rassische und ethnische Herkunft, über Gewerkschaftszugehörigkeit, über religiöse oder philosophische Überzeugung des Betroffenen. Dabei ist eine inhaltliche Auslegung dieser Begriffe im Lichte des BDSG-neu vorzunehmen, soweit sie im diesem Gesetz explizit geregelt. Mithin kann das deutsche Recht auch noch weitere Datenkategorien als besonders schutzwürdig einstufen. Eine Verarbeitung von Daten im Zusammenhang mit Straftaten ist möglich, unterfällt aber meistens besonderen Voraussetzungen des deutschen Rechtes (bspw. der Strafprozessordnung).

Das deutsche Recht muss eine Verarbeitung besonders schutzwürdiger Daten explizit vorschreiben oder erlauben. Eine Verarbeitung der verantwortlichen Stelle kann jedoch auch notwendig sein, um gewissen arbeitsrechtlichen Rechten und Pflichten im Verhältnis der Verantwortlichen Stelle zu ihren Mitarbeiterinnen und Mitarbeitern gerecht zu werden. Diesen ist es im Übrigen unbenommen, freiwillig und ausdrücklich in eine Verarbeitung einzuwilligen.

Bei geplanten Verarbeitungen besonders schutzwürdiger Daten, ist zuvor der Unternehmensbeauftragte für den Datenschutz zu informieren.

f) Telekommunikation

Das Internet, die Telefonanlage(n) und die E-Mail-Adressen als auch der Auftritt in sozialen Netzwerken werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch die Verantwortliche Stelle zur Verfügung gestellt. Deshalb handelt es sich dabei auch um sogenannte Arbeitsmittel und Unternehmensressource. Den Rahmen ihrer Nutzung bestimmt das geltende Recht und die unternehmensinterne IT-Richtlinie bzw. Betriebsordnung. Ist die private Nutzung erlaubt, so sind, soweit einschlägig, insbesondere das Telekommunikationsgesetz und das Fernmeldegeheimnis zu beachten.

Die Verantwortliche Stelle überwacht die genannten Arbeitsmittel nicht generell. Gleichwohl können zur Abwehr von Angriffen auf die unternehmenseigene IT-Infrastruktur Schutzmechanismen an den Übergängen ins das Unternehmens-Netz implementiert werden, mithin Muster von Angriffen analysiert und technisch störende bzw. schädigende Inhalte blockiert werden.

Zudem kann es zu einer zeitlich befristeten Protokollierung der Nutzung des Intranets und Internets, der E-Mail-Adressen, der Telefonanlage(n) und der internen sozialen Netzwerke kommen.

Davon zu trennen ist die personenbezogene Datenauswertung. Diese erfolgt nur bei einem konkreten Verdacht eines Gesetzes- (bspw. §§ 202a, 202 b., 303 b StGB) oder Richtlinienverstoßes (IT-Richtlinie, Betriebsordnung der Verantwortliche Stelle). Eine Kontrollmaßnahme durch den ermittelnden Bereich erfolgt stets entlang des Verhältnismäßigkeitsprinzips und unter Wahrung des deutschen Gesetzes sowie der hierzu getroffenen Regelungen (Compliance-System) der Verantwortlichen Stelle.

6. Übermittlung personenbezogener Daten

Für einige Geschäftsprozesse ist es notwendig, dass personenbezogene Daten von Kunden oder Partnern an Dritte übermittelt werden. Wenn dies nicht aufgrund einer rechtlichen Verpflichtung erfolgt, muss jeweils geprüft werden, ob ein schutzwürdiges Interesse des Betroffenen entgegensteht. Für eine Übermittlung personenbezogener Daten an eine Stelle außerhalb der Unternehmen der afm Gruppe müssen die Voraussetzungen des Punktes 5 erfüllt werden.

Eine Übermittlung an staatliche Einrichtungen oder Behörden erfolgt soweit erforderlich aufgrund jeweils einschlägiger Rechtsvorschriften.

Im Falle einer Datenübermittlung von Dritten an ein Unternehmen der afm Gruppe muss sichergestellt sein, dass die Daten im Rahmen des jeweils geltenden Rechts rechtmäßig erhoben wurden und für die vorgesehene Verarbeitungsmöglichkeiten verwendet werden dürfen.

7. Datenübermittlungen innerhalb der afm Gruppe

Gibt eine rechtlich selbständige Konzerngesellschaft personenbezogene Daten an eine andere Konzerngesellschaft weiter, handelt es sich rechtlich um eine Übermittlung an Dritte. Für eine solche Übermittlung müssen die Voraussetzungen des Punktes 5 gegeben sein.

8. Datenverarbeitung im Auftrag

Bei einer Datenverarbeitung im Auftrag wird ein Dienstleister mit der Durchführung der Datenverarbeitung beauftragt, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Im Falle einer Weitergabe personenbezogener Daten im Rahmen einer

Datenverarbeitung im Auftrag bleibt der Auftraggeber die für die Verarbeitung verantwortliche Stelle. Sämtliche Rechte der Betroffenen sind ihm gegenüber geltend zu machen.

Darüber hinaus sind bei der Auftragserteilung folgende Maßgaben zu befolgen:

1. Bei der Auswahl des Auftragnehmers ist sicherzustellen, dass er die für die Verarbeitung notwendigen technischen und organisatorischen Anforderungen und Sicherheitsmaßnahmen gewährleisten kann.

2. Die Durchführung der Auftragsdatenverarbeitung muss in einem schriftlichen Vertrag geregelt werden, in dem die Anforderungen zum Datenschutz und zur Informationssicherheit vereinbart sind. Insbesondere muss festgelegt werden, dass der Auftragnehmer die Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten darf.

3. Bei der Vertragsgestaltung müssen die Datenschutzrichtlinien beachtet werden.

9. Telekommunikation und Internet

Die Verarbeitung personenbezogener Daten, die bei der Telekommunikation mit dem Betroffenen einschließlich der Internet-Kommunikation anfallen, richtet sich nach den jeweils geltenden Arbeitsanweisungen (u.a. Verhaltensregeln im Rahmen der afm Datenschutzrichtlinie) bzw. nach dem jeweils geltenden Recht.

Konzernstandards zur Umsetzung rechtlicher Vorgaben bei der Gestaltung von Webseiten sind einzuhalten.

10. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind.

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. Der Betroffene ist berechtigt die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten müssen beachtet werden.

5. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Direktwerbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse der verantwortlichen Stelle überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

11. Vertraulichkeit der Verarbeitung

Personenbezogene Daten von Kunden und Partnern werden vertraulich behandelt; eine unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Erforderlich ist dafür ein sogenanntes Berechtigungskonzept des Unternehmens durch das die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten (ähnlich einem Fachbereichsorganigramm) aber auch deren Umsetzung und Pflege klar und transparent geregelt ist.
Insbesondere ist es untersagt, personenbezogene Daten für eigene private oder wirtschaftliche Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen.
Abschließend ist zu beachten, dass auch nach Beendigung des Beschäftigungsverhältnisses die Verpflichtung (des dann ehemaligen Beschäftigten) zur Vertraulichkeit der Daten fortbesteht.

12. Sicherheit der Verarbeitung

Zur Gewährleistung der Datensicherheit sind geeignete technische und organisatorische Maßnahmen implementiert, die auch den Schutz personenbezogener Daten gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung sicherstellen. Sie beziehen sich auf die Sicherheit schutzwürdiger Daten sowohl bei elektronischen Verarbeitungen als auch in Papierform.

Diese technisch-organisatorischen Maßnahmen sind Teil eines integrierten Informationssicherheitsmanagements und werden kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst.

13. Datenschutzkontrolle

Die Verantwortliche Stelle führt regelmäßig sogenannte Datenschutzaudits durch ausgewiesene externe Fachleute bzw. (Fach-)Anwälte für IT-Recht durch. Ziel der weiteren Kontrollen ist es DS-GVO- und BDSG-neu-compliant aufgestellt zu sein.

Die Durchführung dieser Audits wird durch den Datenschutzbeauftragten bzw. durch auf das Datenschutz-Prüfwesen spezialisierte ext. Fachinformatiker und (Fach-)Anwälte für IT-Recht koordiniert und betreut. Alle Ergebnisse und Auswertungen dieser Audits werden dem Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten der Verantwortlichen Stelle gemeldet.

Der zuständigen Datenschutzaufsichtsbehörde (hier: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Klosterwall 6, 20095 Hamburg) wird auf Antrag hin, das jeweilige Ergebnis dieser Datenschutzkontrollen zur Aufsicht übermittelt.

Gleichwohl ist es der zuständigen Datenschutzaufsichtsbehörde unbenommen eigene Audits (Überprüfungen) im gesetzlich abgesteckten Rahmen bei der Verantwortlichen Stelle (Adresse) zwecks Prüfung der Einhaltung dieser Datenschutzrichtlinie vorzunehmen.

14. Datenschutzvorfälle

Alle Beschäftigten der Verantwortlichen Stelle sind dazu angehalten sich der besonderen Bedeutung des Datenschutzes bewusst zu sein. Auch deshalb fordert und fördert die Verantwortliche Stelle von ihren Beschäftigten, wahrgenommene Datenschutzverstöße bzw. Verstöße gegen diese Datenschutzrichtlinie unverzüglich dem jeweils Vorgesetzten (bzw. Weisungsbefugten) zu melden. Die jeweilige Vorgesetztenperson hat den Datenschutzverstoß unverzüglich beim Datenschutzbeauftragten der Verantwortlichen Stelle zu melden.

In den folgenden drei Fällen sind vorgesehene Meldungen als Teil des Information Security Incedent Managements innerhalb der Verantwortlichen Stelle unverzüglich vorzunehmen, um den Meldepflichten des Unternehmens nach dem Recht der Bundesrepublik Deutschland nachkommen zu können.

Den drei erwähnten Fällen werden zugeordnet:

1. die erfolgte unrechtmäßige Übermittlung personenbezogener Daten an Dritte,
2. der unrechtmäßige Zugriff durch einen Dritten auf personenbezogene Daten oder
3. der schlichte Verlust personenbezogener Daten.

15. Verantwortlichkeiten und Sanktionen

Die Vorstände und Geschäftsführungen der Unternehmen der afm Gruppe sind als jeweilige Verantwortliche für die Datenverarbeitung verpflichtet sicherzustellen, dass die gesetzlichen und die in den Datenschutzrichtlinien formulierten Anforderungen des Datenschutzes beachtet werden. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes in ihrem Verantwortungsbereich sicherzustellen.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen nach sich.

16. Der Beauftragte für den Datenschutz

Der Beauftragte für den Datenschutz als internes fachlich weisungsunabhängiges Organ überwacht die Einhaltung der Datenschutzvorschriften. Er ist verantwortlich für die Richtlinien auf dem Gebiet des Datenschutzes und überwacht deren Einhaltung. Er führt Datenschutz-Kontrollen durch. Der Beauftragte für den Datenschutz wird vom Vorstand der afm Holding AG bestellt.

Die Geschäftsführung ist verpflichtet, den Beauftragten für den Datenschutz in seiner Tätigkeit zu unterstützen.

Die Fachbereiche müssen den Datenschutzbeauftragten über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Beauftragte für den Datenschutz schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzbedürftige personenbezogene Daten.
Bei Datenschutzverletzungen und Beschwerden sind die verantwortlichen Führungskräfte verpflichtet, umgehend den Beauftragten für den Datenschutz zu unterrichten. Daneben kann sich jeder Betroffene jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Beauftragten für den Datenschutz wenden. Die Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Die Entscheidungen des Beauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch die Geschäftsführung zu respektieren.

Der Beauftragte für den Datenschutz für die afm assekuranz-finanz-makler GmbH sowie die afm Holding AG kann wie folgt erreicht werden:

afm assekuranz-finanz-makler GmbH
Beauftragter für den Datenschutz
Kaiser-Wilhelm-Straße 9
20355 Hamburg
E-Mail: datenschutz@afm-gruppe.de

I. Anhang

Definitionen

Anonymisierte Daten
Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

Betroffener
Betroffener im Sinne dieser Richtlinie ist jede natürliche Person, über die Daten verarbeitet werden.

Besonders schutzbedürftige Daten
Dabei handelt es sich um Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Ebenso dürfen Daten, die Straftaten betreffen häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

Dritte
Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Ebenfalls Dritte sind Auftragsverarbeiter, die gesetzlich der verantwortlichen Stelle zugeordnet sind.

Einwilligung
Die Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

Erforderlich
Erforderlich ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.

Personenbezogene Daten
Dies sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.
Übermittlung
Die Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

Verarbeitung personenbezogener Daten
Hierbei handelt es sich um jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

Verantwortliche Stelle
Dies ist diejenige juristisch selbständige Gesellschaft, deren Geschäftsaktivität die jeweilige Verarbeitungsmaßnahme veranlasst.

Auswahl gesetzlicher Vorschriften

Im Folgenden möchten wir Ihnen als Mitarbeiter und Adressat umfangreicher gesetzlicher Pflichten eine Auswahl gesetzlicher Vorschriften über das datenschutzrechtliche Regelwerk an die Hand geben, damit Sie sich einen Überblick verschaffen können.

Datenschutzgrundverordnung (DS-GVO)

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „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 mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „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, das Organisieren, das Ordnen, das Speichern, das Anpassen oder Verändern, das Auslesen, das Abfragen, das Verwenden, das Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder das Verknüpfen, das Einschränken, das Löschen oder das Vernichten.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a) DS-GVO: 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").

Art. 5 Abs. 1 lit. f) DS-GVO: Personenbezogene Daten müssen […] 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").

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung

bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Bundesdatenschutzgesetz (n.F.)

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Strafgesetzbuch (StGB)

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Sozialgeheimnis

Sozialgesetzbuch (SGB)

§ 78 Abs. 1 Satz 2 und 3 SGB X: […] 2 Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. 3Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 [SGB I] genannten Stellen.