Richtlinie zum Umgang mit personenbezogenen Daten

in der Deutschen Gesellschaft für Qualität e.V., FQS e.V. und seine Gesellschaften Weiterbildung und Service GmbH

EU-Datenschutzgrundverordnung

Version 1.0

Inhalt

1. Einleitung 3

2. Ziel der Richtlinie 3

3. Anwendungsbereich der Richtlinie 3

4. Grundsätze für die Verarbeitung personenbezogener Daten bei DGQ 4

5. Übermittlung personenbezogener Daten 10

6. Rechte der Betroffenen 11

7. Verfahrensregeln 14

8. Sanktionierung 16

Abkürzungen 17

Begriffsbestimmungen 17

Anlagen 27

1. Einleitung

Für die DGQ sind Informationen und ihre sinnvolle Nutzung zur Verwirklichung der Unternehmensziele von herausragender Bedeutung. Die modernen Informations- und Kommunikationsmedien schaffen eine Basis, um notwendige Unternehmensentscheidungen zeitnah zu planen und effektiv umzusetzen. Die eingesetzten Techniken bergen bei all Ihren innovativen Eigenschaften aber auch Risiken für die Persönlichkeitsrechte der einzelnen Beteiligten. Durch eine unsachgemäße oder missbräuchliche Nutzung der Informationstechnologie und durch die Verarbeitung personenbezogener Daten können Persönlichkeitsrechte verletzt werden.

Um den Anforderungen unserer Mitglieder, Kunden /Teilnehmer, Lieferanten, sonstigen Vertragspartnern und Mitarbeitern an den Schutz Ihrer Persönlichkeitsrechte zu entsprechen, schenkt die DGQ den Anforderungen aus den unterschiedlichen Rechtsordnungen besondere Beachtung.

Der Schutz der Persönlichkeitsrechte jedes Betroffenen, dessen personenbezogene Daten die DGQ verarbeitet, ist das Ziel welches sich die DGQ gesetzt hat. Die Richtlinie wurde erstellt um diesem Ziel gerecht zu werden. Sie ist für alle Unternehmen der DGQ-Gruppe verbindlich. Datenschutz und Datensicherheit ist im Umgang mit Geschäfts- und Personaldaten ein wichtiges Thema. Auf Basis von Datenschutz- und Datensicherheitsmaßnahmen sind wir in der Lage, professionelle und auf Vertrauen basierende Vereinbarungen zu treffen. Es ist uns damit auch möglich, unseren Kunden und Partnern zu zeigen, dass wir bewusst mit den Themen Datenschutz und Datensicherheit umgehen.

Einen wichtigen Teil der Datenschutzmaßnahmen bilden Regeln, welche die Art und Weise, mit der Daten be- und verarbeitet werden, beschreiben (Anlage 1 „Merkblatt zum Datenschutz“). Hierzu gehören die nach § 9 BDSG / Artikel 32 EU-DSGVO geforderten technischen und organisatorischen Maßnahmen (Anlage 2 „Technische und Organisatorische Maßnahmen nach § 9 Anhang BDSG/ Artikel 32 EU-DSGVO“) und die Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf die von unserem Unternehmen definierten Standards (Anlage3). Um den gesetzlichen Anforderungen gerecht zu werden und um unsere Datenverarbeitungsanlagen und Geschäfts- und Personaldaten vor unbefugter Benutzung und vor unberechtigten Zugriffen zu schützen, haben wir diese Richtlinie erstellt.

2. Ziel der Richtlinie

Ziel dieser Richtlinie ist es, Datenschutz- und Datensicherheitsstandards für die Verarbeitung innerhalb der DGQ-Gruppe und die Übermittlung personenbezogener Daten festzulegen. Mit der Festlegung wird ein angemessener Schutz der Persönlichkeitsrechte der Betroffenen sowie Transparenz hinsichtlich der Verarbeitungen gewährleistet. Es wird ein gruppenweites, einheitlich hohes Datenschutzniveau geschaffen. Führungskräfte und Mitarbeiter werden durch die Richtlinie dabei unterstützt, die Anforderungen an den Datenschutz in die jeweiligen Prozesse zu integrieren. Ihre Befolgung ist auch eine Voraussetzung für den Austausch personenbezogener Daten innerhalb der DGQ-Gruppe.

3. Anwendungsbereich der Richtlinie

Diese Richtlinie findet für alle, den Datenschutz betreffenden Fragen Anwendung. Die Richtlinie gilt für die personenbezogenen Daten von Mitarbeitern, Mitgliedern, Kunden, Lieferanten, anderen Geschäftspartnern, sowie Teilnehmern, Interessenten und sonstigen Betroffenen, soweit sie beim der DGQ verarbeitet werden, ungeachtet der Herkunft dieser Daten. Die Datenschutz- und Datensicherheitsstandards dieser Richtlinie sind für alle Unternehmen der DGQ-Gruppe verbindlich.

Sofern ein Unternehmensteil Anlass hat anzunehmen, dass die ihn betreffenden Rechtsvorschriften ihn daran hindern, seinen Verpflichtungen im Rahmen der verbindlichen unternehmensinternen Vorschriften nachzukommen, und dass sie eine wesentliche nachteilige Wirkung auf die durch die Vorschriften gebotenen Garantien haben, wird unverzüglich der jeweils zuständige Geschäftsführer und der Vorstand/die Gesellschafter informiert. Diese treffen dann – beraten durch den Datenschutzbeauftragten der DGQ-Gruppe – eine verantwortliche Entscheidung.

Nicht beherrschte Beteiligungsunternehmen können sich rechtsverbindlich zur Einhaltung der Richtlinie verpflichten. Bei Nichtverpflichtung ist in jedem Einzelfall die Zulässigkeit der Datenübermittlung festzustellen und durch geeignete Maßnahmen sicherzustellen.

Die Erhebung von und Übermittlung personenbezogener Daten an staatliche Einrichtungen erfolgt ausschließlich auf der Grundlage einschlägiger Rechtsvorschriften.

Bestehende gesetzliche Verpflichtungen werden von dieser Richtlinie nicht berührt.

4. Grundsätze für die Verarbeitung personenbezogener Daten bei der DGQ

Der Datenschutz besitzt bei der DGQ einen hohen Stellenwert und ist unternehmensweit organisiert. Dafür wurden zentrale Vorgaben und Richtlinien entwickelt.

Die Gesamtverantwortung für die Einhaltung des Datenschutzes in der DGQ-Gruppe kommt nach EU -DSGVO dem Vorstand sowie für ihren Bereich der Geschäftsführung der Organisationseinheiten zu.

Der Datenschutzbeauftragte der DGQ-Gruppe unterstützt den Vorstand und die Geschäftsführer bei der Einhaltung der gesetzlichen Anforderungen. Er ist in der Ausübung seines Amtes weisungsfrei, dem Vorstand direkt unterstellt und berichtet diesem jährlich. Er wird von DS-Koordinatoren in den einzelnen Organisationseinheiten unterstützt.

Alle beteiligten Bereiche und die Fachressorts regeln entsprechend ihrem Aufgabenfeld, auf Basis der zentralen Vorgaben, die Datenverarbeitung auf ihrem Gebiet. Die Fachverantwortlichen sind verantwortlich für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in Ihrem Bereich. Sie treffen gegebenenfalls zusammen mit den IT-Verantwortlichen entsprechende technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten. Diese werden risikoorientiert ausgerichtet. Das IT-Sicherheitskonzept schreibt die Prozedere vor. In fachspezifischen Datenschutzfragen werden sie jeweils zusätzlich beraten.

4.1 Zulässigkeiten der Datenverarbeitung und Transparenz

Die Verarbeitung personenbezogener Daten unterliegt dem grundsätzlichen Verbot mit Erlaubnisvorbehalt. Die Persönlichkeitsrechte der Betroffenen werden gewahrt.

Personenbezogene Daten müssen auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die Unternehmen der DGQ- Gruppe stellen allen betroffenen Personen angemessene Informationen zur Verarbeitung der personenbezogenen Daten in verständlicher Form zur Verfügung.

Im Umgang mit den personenbezogenen Daten wird eine nachvollziehbare und für jedermann leicht zugängliche Strategie verfolgt.

Werden Daten direkt bei der betroffenen Person erhoben erfolgt diese Information zum Zeitpunkt der Datenerhebung, im Fall einer Erhebung bei einem Dritten spätestens innerhalb eines Monats nach dem Datenerhalt.

Die Betroffenen erhalten Informationen über:

1. Identität und Kontaktdaten des Verantwortlichen, seines Vertreters sowie eines bestellten Datenschutzbeauftragten;
2. die Zwecke, für die die Daten verarbeitet werden sowie bei Zweckänderungen die Rechtsgrundlage der Verarbeitung. Wenn eine Zweckänderung geplant ist, mindestens Informationen über den geänderten Zweck.
3. die Dauer der Speicherung oder die Kriterien für die Festlegung der Speicherdauer;
4. einen Hinweis auf das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragung und Widerspruch gegen die weitere Datenverarbeitung.
5. Wenn Daten bei Dritten erhoben werden, den Hinweis auf die Quelle, aus der die Daten stammen.
6. Wenn Übermittlung stattfinden, die Empfänger oder Kategorien von Empfänger der Daten. Werden Daten in Staaten außerhalb der EU übermittelt, wird die Grundlage für den Datentransfer genannt. Bei vertraglichen Regelungen, die Möglichkeit einer Einsicht in die jeweiligen Vereinbarungen.

7. Wenn eine automatisierte Entscheidungsfindung einschließlich Profiling stattfinden soll, den Hinweis darauf sowie Informationen zu der dabei verwendeten Software-Logik. Weiterhin die Folgen und beabsichtigten Auswirkungen für die betroffene Person,

4.2 Voraussetzungen für die Verarbeitung:

Jede Verarbeitung personenbezogener Daten erfordert einen Erlaubnistatbestand; sie dürfen ausschließlich für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Es wird für jedwede Form der Verarbeitung personenbezogener Daten der Nachweis der Rechtmäßigkeit geführt und dies den Betroffenen gegenüber in nachvollziehbarer Weise dargelegt.

Folgende sechs Erlaubnistatbestände legitimieren die Verarbeitung:

1. *Erfüllung eines Vertrags* (oder eines vertragsähnlichen Vertrauensverhältnisses): Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.
2. *Gesetzliche Grundlage*: Die Verarbeitung ist zur Erfüllung einer Rechtsvorschrift erforderlich, der das Unternehmen der DGQ-Gruppe unterliegt. Kollektivvereinbarungen gelten ebenfalls im Sinne einer Rechtsvorschrift.
3. *Lebenswichtiges Interesse des Betroffenen*: Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.
4. *Öffentliches Interesse*: Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.
5. *Abwägung der Interessen*: Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich, 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.
6. *Einwilligung*: Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.(1)

(1) Es sind die besonderen Anforderungen an eine wirksame Einwilligung und der besondere Schutz von Kindern zu beachten.

Voraussetzungen für die wirksame Einwilligung

Die Einwilligung wird nur bei fehlender gesetzlicher Grundlage eingeholt.

Die Einwilligung muss als solche äußerlich sofort erkennbar sein und erkennbar von anderen Sachverhalten getrennt werden. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Die Möglichkeit des Widerrufs ist so einfach gestaltet, wie Abgabe der Einwilligung.

Stützt sich die Datenverarbeitung auf eine Einwilligung, so muss diese in schriftlicher oder in elektronischer Form dokumentiert und vom Verantwortlichen nachgewiesen werden können.

Die Einwilligung

1. erfolgt freiwillig und ohne Zwang.
2. ist vor Beginn der Verarbeitung schriftlich oder auf andere rechtlich zulässige Art eingeholt (z.B. elektronisch)
3. kann nachgewiesen werden (Dokumentationspflicht)
4. ist zur Verdeutlichung gegenüber anderen Erklärungen optisch hervorgehoben.
5. ist nicht in unzulässiger Weise mit weiteren Einwilligungen gekoppelt
6. Bezieht sich, bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Nr. 2 a) DSGVO) ausdrücklich auf diese Daten.
7. Die mögliche Übermittlung an Dritte wird beschrieben.
8. Im Bereich elektronischer Medien besteht mindestens ein sog. Opt-In Verfahren.
9. Die Einwilligung ist klar und deutlich abgefasst. Sie beschreibt hinreichend, möglichst konkrete und klar umgrenzte Tatbestände. z.B.: Abschließende Aufzählung der Empfänger, bei Übermittlung der Daten, exakte Löschfristen

10. Die Betroffenen sind vor der Einwilligung auf den vorgesehenen konkreten Zweck der Verarbeitung in einfacher, klarer und angemessener Sprache hingewiesen.
11. Die Betroffenen sind über mögliche Folgen der Verweigerung der Einwilligung aufgeklärt.
12. Der Einwilligung kann jederzeit, mit Wirkung für die Zukunft widersprochen werden. Der Widerruf ist in der gleichen, einfachen Weise möglich, wie die Zustimmung.
13. Die Betroffenen sind vor Ihrer Einwilligung auf ihr Widerrufsrecht aufmerksam gemacht.
14. Die Betroffenen sind auf ihr Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragung hingewiesen.
15. Die Betroffenen sind auf ihr Beschwerderecht bei der Aufsichtsbehörde hingewiesen.
16. Einwilligung von Minderjährigen unter 16 Jahren sind mit der Zustimmung des Trägers der elterlichen Verantwortung oder durch ihn erteilt. Die Formulierung der Einwilligung ist in einfacher und verständlicher Sprache gehalten und entspricht dem Alter der Betroffenen.

Bei Unklarheiten bezüglich der Zulässigkeit der Datenverarbeitung stehen die Datenschutzkoordinatoren bzw. der Datenschutzbeauftragte zur Verfügung.

4.3 Zweckbindung

Personenbezogene Daten werden nur für genau festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet. Die Verarbeitung und Nutzung ist dem Zwecke angemessen und sachlich relevant. Die Daten werden nicht in einer mit dieser Zweckbindung unvereinbaren Weise weiterverarbeitet. Die Zweckbestimmung der von einer anderen Stelle oder DGQ Organisationen oder Unternehmen der DGQ Gruppe? übermittelten Daten ist vom Empfänger bei ihrer weiteren Nutzung und Speicherung zu beachten. Jede Zweckänderung wird zum Nachweis der Rechtmäßigkeit dokumentiert.

4.4 Datenminimierung

Die Verarbeitung personenbezogener Daten muss sachlich relevant, dem Zweck der Wahrung berechtigter Interessen angemessen und auf das für die Zwecke

der Verarbeitung notwendige Maß beschränkt sein. Es werden nur so wenig personenbezogene Daten wie möglich, also nur die zur jeweiligen Aufgabenerfüllung notwendigen, personenbezogenen Daten, verarbeitet. Sie werden frühzeitig anonymisiert bzw. pseudonymisiert. Die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel ausgerichtet, so wenig personenbezogene Daten wie möglich zu verarbeiten.

4.5 Datenqualität

Personenbezogene Daten müssen sachlich richtig und – wenn notwendig – auf dem neuesten Stand sein. Unzutreffende, unvollständige oder nicht mehr benötigte Daten sind zu berichtigen oder zu löschen. Daten, die nicht mehr benötigt werden sind unter Beachtung vorgeschriebener Aufbewahrungsfristen zu löschen/ bzw. zu sperren. Hierfür sind angemessene Maßnahmen zu ergreifen.

4.6 Sicherheit der Datenverarbeitung: Integrität, Verfügbarkeit und Vertraulichkeit

Personenbezogene Daten werden in einer Weise verarbeitet, die einen angemessenen Schutz der Daten gewährleistet. Die vorgeschriebene Datensicherheit umfasst auch den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung durch entsprechend geeignete technische und organisatorische Maßnahmen.

Die verantwortlichen Stellen haben zur Gewährleistung der erforderlichen Datensicherheit angemessene technische und organisatorische Maßnahmen zu treffen. Diese Vorkehrungen beziehen sich auf alle Verarbeitungssysteme. Die zu treffenden Maßnahmen sind im IT-Sicherheitskonzept definiert. Sie werden im Hinblick auf die Art, den Umfang der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere

der Risiken für die Rechte und Freiheiten risikoorientiert umgesetzt.

Die Maßnahmen sind im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

4.7 Verletzungen des Schutzes personenbezogener Daten

Bei Verletzungen des Schutzes personenbezogener Daten werden die gesetzlichen Melde- und Benachrichtigungspflichten eingehalten.

Nach Bekanntwerden von Verletzungen des Schutzes personenbezogener Daten werden umgehend die Geschäftsleitung und der Datenschutzbeauftragte informiert.

Eine Meldung an die Aufsichtsbehörde hat immer zu erfolgen, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko" für den Betroffenen führt. Es wird hierfür vom Verantwortlichen eine Risikoabwägung durchgeführt.

Die Meldung an die Aufsichtsbehörde erfolgt innerhalb 72 Stunden. Ein Überschreiten der Frist ist nur in begründeten Fällen möglich. Die Meldung umfasst u. a. die Art der Datenpanne, die Kategorien von betroffenen Daten, die Anzahl der Betroffenen und der Datensätze, eine Einschätzung der Folgen für den Betroffenen sowie die Maßnahmen zur Ursachenbeseitigung bzw. zur Schadensminimierung beim Betroffenen.

Eine Information des Betroffenen ist nicht erforderlich, wenn geeignete technische und organisatorische Maßnahmen vorhanden sind, die den Unbefugten Zugang auf die personenbezogenen Daten praktisch nicht ermöglichen (z.B.: Verschlüsselung). Ebenso kann auf eine Benachrichtigung des Betroffenen verzichtet werden, wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden und diese das hohe Risiko, das zum Zeitpunkt der Datenpanne bestand, eliminiert haben.

4.8 Speicherbegrenzung und Richtigkeit der Daten

Personenbezogene Daten dürfen nur verarbeitet werden, solange dies für die Verwirklichung der mit der Verarbeitung verfolgten Zwecke erforderlich ist. Danach sind sie zu löschen oder insofern Aufbewahrungspflichten bestehen, zu sperren, das heißt, mit restriktiven Zugriffsrechten in verschlüsselter Form in gesondertem Bereich gehalten werden.

Daten sind ebenfalls zu löschen, bei widerrufener Einwilligung, wenn die betroffene Person Einspruch gegen die Verarbeitung einlegt oder die Daten unrechtmäßig verarbeitet wurden. Die für die Daten Verantwortlichen legen jeweils unter Beachtung der Aufbewahrungspflichten, Fristen für die regelmäßige Überprüfung oder Löschung fest.

4.9 Besondere Kategorien personenbezogener Daten (besonders sensible Daten)

Besonderer Kategorien personenbezogener Daten sind:

- Angaben über rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit und Sexualleben
- Genetische und Biometrische Daten
  Der Missbrauch besonderer Kategorien personenbezogener Daten kann die Existenz, Gesundheit, Leben oder die Freiheit des Betroffenen erheblich beeinträchtigen. Diese Daten entsprechen in der DGQ-Gruppe der Schutzstufe 3 und erfahren entsprechend besonderen Schutz. (siehe Kapitel 1.3 Definition der Daten-Schutzklassen/-stufen in der Leitlinie zur Informationssicherheit).

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist grundsätzlich verboten. Sie kann nur unter eng begrenzten gesetzlichen Erlaubnistatbeständen durchgeführt werden.

Solche Verarbeitungen müssen im Vorfeld seitens der Verantwortlichen generell einer risikoorientierten Datenschutzfolgeabschätzung unterzogen werden. Das Ergebnis ist zu dokumentieren. Die Verantwortlichen können bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten einholen.

4.10 Datenschutzfolgeabschätzung

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Datenschutzfolgeabschätzung). Eine Datenschutzfolgeabschätzung durch die Verantwortlichen ist insbesondere durchzuführen,

1. wenn besondere Kategorien personenbezogener Daten verarbeitet werden oder
2. bei Verarbeitungen mit neuen Technologien und neuen Verarbeitungen zu denen bisher keine Datenschutzfolgeabschätzung durchgeführt wurden.

Bei der Datenschutzfolgeabschätzung werden folgende Punkte berücksichtigt:

1. Vorgaben der Aufsichtsbehörden
2. Ähnliche Verarbeitungsvorgänge
3. Beteiligung des Datenschutzbeauftragten
4. Systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke inklusive dem verfolgten Interesse
5. Verhältnismäßigkeitsprüfung
6. Maßnahmen zu Risikoverringerung
7. Gegebenenfalls Abstimmung mit betroffenen Personen
8. Feststellungen zu späteren Überprüfungen
9. Abschließende Risikobewertung
10. Feststellungen zur Konsultationspflicht der Aufsichtsbehörde

Die Verantwortlichen Fachbereiche können bei der Erstellung von Datenschutzfolgeabschätzung den Datenschutzbeauftragten beratend hinzuziehen.

4.11 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung ist in schriftlicher oder elektronischer Form, auch zu Nachweiszwecken durchzuführen (Siehe auch: "**Voraussetzungen für die wirksame Einwilligung" Art. 7 Abs. 1 DSGVO)**. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht in Textform aufzuklären.

4.12 Bereitstellung betrieblicher Adress-, Funktions- und Kommunikationsdaten

Für Zwecke der innerbetrieblichen Kommunikation ist die Bereitstellung betrieblicher Adress-, Funktions- und Kommunikationsdaten der Beschäftigten – z.B. über das Intranet – innerhalb der DGQ-Gruppe zulässig, soweit diese Daten zur Erfüllung der betrieblichen Tätigkeit erforderlich sind. Dabei ist die Zweckbindung der Daten von allen Nutzern zu beachten.

4.13 Auftragsverarbeitung

Wenn Unternehmen der DGQ-Gruppe oder sonstige externe Unternehmen im Rahmen eines Auftragsverhältnisses zur Verarbeitung personenbezogener Daten als Auftraggeber oder Auftragsnehmer (Auftragsverarbeiter) fungieren, gilt Folgendes:

1. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutzgesetzgebung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
2. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
3. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten. Der Vertrag ist schriftlich abzufassen. Dies kann auch in elektronischer Form erfolgen. In diesem Vertrag bzw. diesem anderen Rechtsinstrument werden mindestens folgende Punkte geregelt:
    1. Gegenstand und Dauer des Auftrags
    2. Konkretisierung des Auftragsinhalts
    3. Technisch-organisatorische Maßnahmen
    4. Berichtigung, Einschränkung und Löschung von Daten
    5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers
    6. Unterauftragsverhältnisse
    7. Kontrollrechte des Auftraggebers
    8. Mitteilung bei Verstößen des Auftragnehmers
    9. Weisungsbefugnis des Auftraggebers
    10. Löschung und Rückgabe von personenbezogenen Daten

Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.

Die zentrale Rechtsabteilung stellt entsprechende Musterverträge zur Verfügung. Verträge zur Auftragsverarbeitung werden vor Abschluss durch Juristen abschließend geprüft.

4.14 Automatisierte Einzelentscheidungen

Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

4.15 Dokumentation der Verfahren

Vor Inbetriebnahme neuer und bei Änderung vorhandener Verarbeitungstätigkeiten werden diese von den Verantwortlichen für die Verarbeitung für das Verzeichnis der Verarbeitungstätigkeiten dokumentiert. Das Verzeichnis wird dem Datenschutzbeauftragten zur Verfügung gestellt. Der Datenschutzbeauftragte/die Datenschutzkoordinatoren erhalten in der Praxis die Informationen unaufgefordert von den Verantwortlichen der jeweils zuständigen Fachbereiche.

Bestandteile der Dokumentation:

1. Bezeichnung der Verarbeitungstätigkeit
2. Name oder Firma der verantwortlichen Stelle, gegebenenfalls der gemeinsam Verantwortlichen.

3. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
4. Bereitgestellter Datenschutzbeauftragter (Name, Funktion, E-Mail-Adresse, Telefonnummer)
5. Anschrift der verantwortlichen Stelle, gegebenenfalls der gemeinsam Verantwortlichen
6. Bezeichnung der für die Verarbeitung Verantwortlichen (Fachlich und Technisch)
7. Zweckbestimmungen der Verarbeitung
8. Rechtsgrundlage der Verarbeitungen/Verarbeitungstätigkeiten
9. Eine Beschreibung der betroffenen Kategorien der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien, gegebenenfalls der besonderen Kategorien personenbezogener Daten.
10. Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt werden
11. Regelfristen für die Löschung der Daten,
12. Gegebenenfalls Datenübermittlung in Drittländer oder internationale Organisationen sowie Namen der Drittländer
13. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
14. Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.
15. Zugriffsberechtigte Personen / Personengruppen
16. Angaben zur Technik des Verfahrens
17. Angaben zur Auftragsverarbeitung
18. Gegebenenfalls Angaben zur durchgeführten Datenschutzfolgeabschätzung

In Fällen in denen Unternehmen DGQ als Auftragsverarbeiter fungieren werden

1. die Namen und Kontaktdaten des Auftragsverarbeiters, des Verantwortlichen sowie gegebenenfalls der gemeinsam Verantwortlichen des etwaigen Vertreters und des Datenschutzbeauftragten
2. die Kategorien von verarbeiteten personenbezogenen Daten, die im Auftrag des Verantwortlichen verarbeitet werden
3. die getroffenen technischen und organisatorischen Maßnahmen
4. Gegebenenfalls die Datenübermittlung in Drittländer oder internationale Organisationen sowie Namen der Drittländer

dokumentiert.

5. Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten innerhalb des Europäischen Wirtschaftsraums (EWR[2]) ist grundsätzlich erlaubt, wenn auch ihre Verarbeitung nach Ziffer 4.1 zulässig ist.

Bei der Übermittlung personenbezogener Daten innerhalb des Landes, in dem sie erhoben wurden, sind die in diesem Land bestehenden gesetzlichen Verpflichtungen zu erfüllen.

5.1 Übermittlung innerhalb der DGQ-Gruppe

Der DGQ-Gruppeninterne Datenaustausch für interne Verwaltungszwecke ist als „berechtigtes Interesse“ erlaubt, wenn nach Interessensabwägung das berechtigte Interesse die schutzwürdigen Interessen der Betroffenen überwiegt.
Bezüglich der Beschäftigtendaten wird auf Punkt: 4.10 dieser Richtlinie verwiesen.

5.2 Übermittlung in Drittstaaten

Eine Datenübertragung personenbezogener Daten in Länder außerhalb des EWR ist nicht vorgesehen. Sollten dennoch personenbezogene Daten in Drittländer übermittelt werden ist dieses nur im Rahmen gesetzlicher Erlaubnistatbestände genehmigt. Der Datenschutzbeauftragte ist mit einzubeziehen.

(Für den Transfer an angehörige Unternehmen in Drittstaaten gelten die Anforderungen der Art. 44 ff. EU-DSGVO (vgl. Erwägungsgrund 48 Satz 2 EU-DSGVO). Hier werden sich Binding Corporate Rules (BCR) regelmäßig als Gestaltungsmittel anbieten, deren Aufstellung in Art. 47 EU-DSGVO geregelt ist.)

6. Rechte der Betroffenen

6.1 Transparenz

Bei der Erhebung personenbezogener Daten bei betroffenen Personen wird ihnen folgendes mitgeteilt:

1. Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
2. Gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
3. Die Zwecke der Verarbeitung
4. Die Rechtsgrundlage der Verarbeitung (Bei Interessensabwägung die Interessen die verfolgt werden)
5. Gegebenenfalls die Empfänger oder Kategorien der Empfänger der Daten
6. Gegebenenfalls die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation
7. Die Dauer für die die Daten gespeichert werden oder die dafür zugrundliegenden Kriterien.
8. *Im Fall einer Zweckänderung wird diese und die obenstehenden Angaben dem Betroffenen ebenfalls mitgeteilt.*
9. Das Bestehen eines Rechts auf:
   - Auskunft seitens des Verantwortliche
   - Berichtigung, Löschung und Einschränkung
   - Wiederspruch gegen die Verarbeitung
   - Datenübertragbarkeit
   - Beschwerderecht bei der Aufsichtsbehörde
10. Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss erforderlich ist.
11. Ob der Betroffene verpflichtet ist, die Daten bereitzustellen und welche möglichen Folgen die Verweigerung hätte

Die Information der betroffenen Person wird dokumentiert.

Werden personenbezogene Daten nicht bei der betroffenen Person selbst erhoben, werden ihr grundsätzlich folgende Informationen bereitgestellt:

1. Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
2. Gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
3. Die Zwecke der Verarbeitung
4. Die Rechtsgrundlage der Verarbeitung (Bei Interessensabwägung die Interessen die verfolgt werden)
5. Gegebenenfalls die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden.
6. Gegebenenfalls die Empfänger oder Kategorien von Empfängern
7. Gegebenenfalls die Absicht, die Daten in ein Drittland oder eine internationale Organisation zu Übermitteln.
8. Die Dauer der Speicherung oder, falls dies nicht möglich, die Kriterien für die Festlegung der Dauer.
9. Woher die Daten stammen und gegebenenfalls ob sie öffentlich zugänglicher Quellen entstammen.

6.2 Auskunftsrecht

Jeder Betroffene hat das Recht zu erfahren, ob von einem der Gruppe zugehörigen Unternehmen personenbezogenen Daten verarbeitet werden. Wenn ja, erhält der Betroffene unverzüglich, spätestens jedoch innerhalb eines Monats Informationen welche Daten dies genau sind sowie

1. über die Verarbeitungszwecke,
2. über die Kategorien personenbezogener Daten, die verarbeitet werden,
3. über die gegebenen oder möglichen Datenempfänger bzw. Kategorien von Empfängern,
4. soweit möglich über die geplante Speicherdauer,
5. Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie über ein Widerspruchsrecht,

6. über das Beschwerderecht bei der Aufsichtsbehörde,
7. über die Herkunft der Daten, soweit diese nicht von der betroffenen Person selbst erhoben wurden,
8. soweit zutreffend über das Bestehen einer automatisierten Entscheidungs-findung einschließlich Profiling.

Die Auskunft erfolgt schriftlich, elektronisch oder mündlich, möglichst in Form einer Kopie der personenbezogenen Daten. Die Auskunft ist zu dokumentieren.

Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er zusätzliche Informationen zur Bestätigung der Identität nachfordern.

Die Auskunft ist unentgeltlich.

Bei Übermittlungen an „Sicherheitsbehörden" bedarf eine Auskunftserteilung der Zustimmung dieser Behörden, außerdem muss sie unterbleiben, falls dies rechtliche Vorschriften fordern.

Um eine vertrauensvolle Zusammenarbeit zu fördern und zu garantieren, sowie unnötige Missverständnisse und damit verbundenen Aufwand und womöglich Schaden zu vermeiden, sollten die Verantwortlichen für die Datenverarbeitung ausdrücklich die Beachtung dieser Rechte und Pflichten fordern und für den Fall einer Anfrage oder Beanstandung ein einfaches Verfahren bereithalten:

Ablauf der Bearbeitung von Anfragen zu gespeicherten Daten

1. von Mitarbeitern

a) Information an den Datenschutzkoordinator (DSK) bzw. den Datenschutzbeauftragten (DSB)
b) Erhebung der dezentral und zentral gehaltenen Daten des MA
c) Beantwortung der Anfrage und Information an DSK und DSB spätestens innerhalb von 14 Tagen nach Eingang der Anfrage.

2. von Teilnehmern/Kunden/weiteren Betroffenen

a) Eingang der Anfrage am Standort
b) Weiterleitung an die zuständige Führungskraft (GF).
c) Information an den Datenschutzkoordinator (DSK) bzw. den Datenschutzbeauftragten (DSB) durch die Geschäftsführung (GF)
d) Schriftliche Mitteilung (Eingangsbestätigung) an den Antragsteller. (gegebenenfalls Nachfrage beim Antragsteller nach Konkretisierung der Daten). (GF)
e) Erhebung der gehaltenen Daten des Betroffenen (GF).
f) Beantwortung der Anfrage und Information an DSK und DSB spätestens innerhalb von 14 Tagen nach Eingang (GF).

6.3 Berichtigungsanspruch

Die betroffene Person hat das Recht, unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

6.4 Widerspruchsrecht

Wenn die Verarbeitung zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** stattfindet, hat die betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung **nachweisen**, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

6.5 Ablehnung des Auskunfts- oder Berichtigungsverlangens

Bei Ablehnung des Auskunfts- oder Berichtigungsverlangens wird dem Betroffenen der Grund hierfür mitgeteilt.

6.6 Recht auf Löschung

1. Die betroffene Person hat das Recht, zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

   a. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
   b. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
   c. Im Fall, dass die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen, oder die betroffene Person legt Widerspruch gegen die Verarbeitung zur Direktwerbung ein.
   d. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
   e. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

2. Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

3. Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

   a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
   b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
   c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin sowie Artikel 9 Absatz 3;
   d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
   e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

6.7 Verwendung von Daten zu Werbezwecken und Widerspruchs recht

Grundlage für die Beurteilung der Zulässigkeit von Werbung ist, abgesehen von einer Einwilligung, eine Interessenabwägung. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

1. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.
2. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.
3. Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

Die Verarbeitung besonderer Kategorien von personenbezogener Daten zu Werbezwecken ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person möglich.

Kopplungsverbot

Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist.

Generell gelten bei Verarbeitungen zu Werbezwecken die Regeln zur Transparenz in dieser Richtlinie.

7. Verfahrensregeln

7.1 Umsetzung in der DGQ-Gruppe

Die Unternehmen der DGQ-Gruppe haben als verantwortliche Stelle zu gewährleisten, dass die in dieser Unternehmensrichtlinie niedergelegten Grundsätze beachtet werden.

Den Mitarbeitern wird ergänzend zu dieser Richtlinie ein Datenschutzhandbuch mit detaillierten Anleitungen zum Verhalten und festgelegten Verantwortlichkeiten zu Verfügung gestellt.

Der Vorstand und die Geschäftsführungen der einzelnen Unternehmen der DGQ-Gruppe haben die Umsetzung dieser Richtlinie sicherzustellen. Hierzu gehört vor allem die entsprechende Unterrichtung der Mitarbeiter. Die Beschäftigten werden entsprechend Schulungsplan mit den Anforderungen des Datenschutzes vertraut gemacht. Bei weiterem Schulungsbedarf wenden sie sich an den Datenschutzkoordinator oder den Datenschutzbeauftragten. Zur Unterrichtung zählt auch der Hinweis, dass Verstöße gegen die Grundsätze dieser Richtlinie unter Umständen straf-, haftungs- oder arbeitsrechtliche Konsequenzen nach sich ziehen können.

7.2 Datenschutzbeauftragter

Der Vorstand berät mit den Geschäftsleitungen der DGQ-Gruppe die Besetzung und benennt einen Datenschutzbeauftragten (DSB) für die DGQ-Gruppe. Der Datenschutzbeauftragte ist für alle Organisationseinheiten zuständig

Der Datenschutzbeauftragte ist in seiner Funktion frei von Weisungen und direkt dem Vorstand unterstellt. Er ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden.

Die Benennung und die Kontaktdaten des Datenschutzbeauftragten werden der Aufsichtsbehörde mitgeteilt. Die Kontaktdaten werden ohne Namensnennung veröffentlicht. Es wird sichergestellt, dass der Konzerndatenschutzbeauftragte aus allen Organisationseinheiten leicht erreichbar ist.

Die Führungskräfte in der DGQ-Gruppe sind verpflichtet, den Datenschutzbeauftragten und die Datenschutzkoordinatoren bei ihrer Tätigkeit zu unterstützen und ihnen insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Bei Fragen oder Unklarheiten zum Datenschutz stehen die Datenschutzkoordinatoren und der Datenschutzbeauftragte für Auskünfte zur Verfügung.

Der Datenschutzbeauftragte ist unter der E-Mail-Adresse: Datenschutzbeauftragter@dgq.de zu erreichen.

7.3 Aufgaben des Datenschutzbeauftragten:

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten
- Überwachung der Einhaltung der EU-DSGVO und nationalen Sonderregelungen
- Beratung und Überwachung im Zusammenhang mit der Datenschutzfolgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde

7.4 Fragen und Beschwerden/Rechtsbehelfe

Betroffene und Beschäftigte können sich mit Fragen oder Beschwerden zur Verarbeitung personenbezogener Daten jederzeit an die Datenschutzkoordinatoren oder an den Datenschutzbeauftragten wenden. Die Anliegen werden vertraulich behandelt.

7.5 Verpflichtung gegenüber Datenschutzaufsichtsbehörden

Der Datenschutzbeauftragte ist verpflichtet, bei allen Anfragen der Datenschutzaufsichtsbehörde, mit ihr zu kooperieren und ihre Feststellungen zu respektieren.

7.6 Benachrichtigungspflicht bei Sicherheitspannen

Die Unternehmen sind verpflichtet, bei bestimmten Arten von Sicherheitspannen, umgehend sowohl die zuständige Datenschutzbehörde als auch gegebenenfalls die natürlichen Personen zu informieren, die von der Sicherheitspanne betroffen sind. Die Benachrichtigungspflicht besteht immer dann, wenn

- der Schutz personenbezogener Daten verletzt wurde und
- Risiken für die persönlichen Rechte und Freiheiten natürlicher Personen bestehen.

also unrechtmäßig übermittelt oder auf sonstige Weise einem Dritten unrechtmäßig zur Kenntnis gelangt sind. Ein Prozess zur Benachrichtigung ist etabliert.

Nach einer Datenpanne müssen der Vorfall und die Umstände die zur Datenpanne führten technisch und organisatorisch beseitigt werden. Weiterhin ist die Angelegenheit zu dokumentieren. Begleitend ist abzuwägen, ob eine Meldung an die Aufsichtsbehörde und gegebenenfalls an die Betroffenen erfolgen muss.

Im Falle einer Datenpanne sind umgehend der Datenschutzbeauftragte und die jeweilige Geschäftsführung zu informieren.

Die Benachrichtigung an die Aufsichtsbehörde hat binnen 72 Stunden erfolgen,

Die Benachrichtigung enthält dann:

1. Eine Beschreibung der Art der Verletzung, Kategorien und Zahl der betroffenen Personen und der Datensätze,
2. Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle und
3. eine Beschreibung der wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Die Benachrichtigung an die Betroffenen erfolgt innerhalb einer angemessenen Frist und enthält:

1. Eine Beschreibung der Art der Verletzung,
2. Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
3. eine Beschreibung der wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Die Meldung erfolgt in klarer und einfacher Sprache.

Besteht ein kein oder nur ein geringes Risiko für die Rechte und Freiheiten der Betroffenen, kann die Benachrichtigung an sie ausbleiben. Die Aufsichtsbehörde kann – nach erfolgter eigener Risikoeinschätzung – das Unternehmen durch Beschluss anweisen, die Meldung an die Betroffenen nachzuholen.

Dokumentation der Pannen/ Sicherheitsvorfälle

Es sind alle zusammenhängenden Fakten, die Auswirkungen und die ergriffenen Maßnahmen zu dokumentieren.

7.7 Evaluation Datenschutz

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen oder beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen sind dem Beauftragten für den Datenschutz mitzuteilen. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zu stehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

7.8 Änderungen der Richtlinie und Fortgeltung

Die DGQ behält sich das Recht vor, diese Richtlinie bei Bedarf zu ändern, etwa um geänderte Anforderungen von Gesetzen, Verordnungen, Forderungen von Datenschutzbehörden oder Unternehmens-internen Verfahren zu entsprechen. Soweit gesetzlich erforderlich, wird die DGQ die etwaig geänderte Unternehmensrichtlinie zur erneuten Überprüfung vorlegen. Tritt diese Richtlinie außer Kraft, wird möglichst umgehend eine aktualisierte Regelung in Kraft gesetzt.

7.9 Publizität

Die jeweils aktuelle Version dieser Richtlinie wird den Beschäftigten in geeigneter Weise zugänglich gemacht.

7.10 Verhältnis zu anderen Unternehmensregelungen

Soweit andere Unternehmensregelungen zum Datenschutz dieser Richtlinie widersprechen, haben die Regelungen dieser zentralen Richtlinie Vorrang.

8. Sanktionierung

Vorsätzliche oder wiederholte Verstöße gegen diese Richtlinie können zu disziplinarischen Maßnahmen führen. Bei besonders schweren Verstößen behält sich das Unternehmen eine Kündigung des Anstellungsverhältnisses vor. Schadensersatzansprüche oder strafrechtliche Maßnahmen werden dadurch nicht eingeschränkt.

ABKÜRZUNGEN

DS	Datenschutz
DSB	Datenschutzbeauftragter
DSF	Datenschutzfolgeabschätzung
DSK	Datenschutzkoordinator
EU-DSGVO	Europäische Datenschutzgrundverordnung
EWR	Europäischer Wirtschaftsraum
GF	Geschäftsführung
IT	Informationstechnologie
PL	Personalleitung

BEGRIFFSBESTIMMUNGEN

Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

Anonymisierung – das Verändern von Daten derart, dass kein Personenbezug mehr herstellbar ist.

Auftragsverarbeiter – jede natürliche oder juristische Person, die personenbezogene Daten im Auftrag für eine verantwortliche Stelle verarbeitet.

Datenschutzbeauftragter – eine Person, die offiziell für ein konzern-angehöriges Unternehmen bestellt wurde, um die innerbetriebliche Datenschutzkontrolle wahrzunehmen, an die Geschäftsführung berichtet und in seiner Funktion nicht weisungsgebunden ist.

Betroffener – jede natürliche Person, deren personenbezogene Daten im Unternehmen verwendet werden, beispielsweise jetzige, künftige und ehemalige Mitarbeiter, Kunden, Lieferanten, Probanden und Patienten in klinischen Prüfungen sowie in sonstigen Vertragsverhältnissen zum Unternehmen stehende natürliche Personen.

Datenschutzkoordinator – eine Person, die für ein konzernangehöriges Unternehmen benannt wurde (Vollmacht), um den Datenschutzbeauftragten zu unterstützen, an ihn berichtet und in seiner Funktion nicht weisungsgebunden ist.

Datenschutz – die Summe aller Maßnahmen zur Wahrung der Persönlichkeitsrechte von Betroffenen im Umgang mit ihren personenbezogenen Daten.

Dritter – jede natürliche oder juristische Person, die nicht der verantwortlichen Stelle zuzurechnen ist, wie z. B. externe Geschäftspartner oder andere Gesellschaften im Unternehmensverbund, nicht jedoch der Betroffene selbst oder der Auftragnehmer bei einer Auftragsdatenverarbeitung innerhalb des Europäischen Wirtschaftsraums (EWR)

Einwilligung – jede ohne Zwang und in Kenntnis der Sachlage erfolgte Willensäußerung, mit der der Betroffene akzeptiert, dass ihn betreffende personenbezogene Daten verarbeitet werden.

Interessenabwägung – Interessenabwägung bedeutet, dass die berechtigten Interessen der verantwortlichen Stelle gegen die schutzwürdigen Interessen des Betroffenen abzuwägen sind.

Opt-In Verfahren – ist ein ausdrückliches Zustimmungsverfahren bei dem der Betroffene sein Einverständnis explizit bestätigen muss.

Personenbezogene Daten – alle persönlichen und sachlichen Informationen über eine bestimmte oder bestimmbare natürliche Person (Betroffener). Bestimmbar ist eine Person dann, wenn sie direkt oder indirekt identifiziert werden kann, z. B. durch Zuordnung einer Kennziffer.

Pseudonymisierung – das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen für Unbefugte auszuschließen oder wesentlich zu erschweren.

Persönlichkeitsrechte – Formen des allgemeinen Persönlichkeitsrechts sind z.B. der Schutz der Privatsphäre, das Recht am eigenen Bild, das Recht auf informationelle Selbstbestimmung. Besondere Persönlichkeitsrechte sind z.B. das Urheberrecht oder das Namensrecht.

Sensitive Daten (Besondere Kategorien personenbezogener Daten) – Angaben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, Genetische und biometrische Daten.

Sozialdaten – Einzelangaben über die persönlichen und sachlichen Verhältnisse (personenbezogene Daten), die von den sozialrechtlichen Leistungsträgern zur Erfüllung ihrer gesetzlichen Aufgaben verarbeitet werden.

Übermittlung personenbezogener Daten – die Weitergabe personenbezogener Daten, ihre Verbreitung oder jede andere Form der Bereitstellung an Dritte, dazu gehören auch die Einsicht in und der Abruf von Informationen.

Verantwortlicher für die Datenverarbeitung (verantwortliche Stelle) – das juristisch selbstständige Unternehmen der DGQ-Gruppe, das über die Verarbeitung personenbezogener Daten entscheidet.

Verarbeitung personenbezogener Daten – jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Prozess in Verbindung mit personenbezogenen Daten wie das Erheben, Speichern, Verändern, Bereitstellen, Übermitteln, Offenlegen, Sperren, Löschen oder Archivieren.

Verarbeitung – Gegenstand einer Verarbeitung ist eine "Datenverarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen". Entscheidend ist die gemeinsame Zweckbestimmung. Eine Verarbeitung in diesem Sinne kann also durchaus eine Vielzahl von Datenverarbeitungsdateien umfassen.

Datenschutzfolgeabschätzung (DSF) – Maßnahme zur Sicherstellung der Recht- und Ordnungsmäßigkeit der Verfahren. Die DSF wird regelmäßig durchgeführt, wenn Verarbeitungen personenbezogener Daten

[2] Der EWR umfasst die Mitgliedsstaaten der Europäischen Union, Island, Liechtenstein und Norwegen.

Gender-Hinweis: Die verwendete maskuline bzw. feminine Sprachform dient der leichteren Lesbarkeit und meint immer auch das jeweils andere Geschlecht.

ANLAGE 1

„DATENSCHUTZ AUF EINEN BLICK“ (SIEHE SEPARATE PDF-DATEI)

ANLAGE 2 Technische und organisatorische Maßnahmen nach § 9 Anhang BDSG / Artikel 32 EU-DSGVO

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, um die in Art. 32 EU-DSGVO verankerten Schutzziele

- **Vertraulichkeit**, d.h. Daten sind für unberechtigte Dritte nicht zugänglich
- **Integrität**, d.h. Daten können nicht verfälscht werden
- **Verfügbarkeit**, d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden

basierend auf den in der Anlage des § 9 BDSG aufgeführten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht

Übersicht TOM´s nach § 9 Anhang BDSG / Artikel 32 EU-DSGVO	
⇨ **Zugangskontrolle** Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte	⇨ **Datenträgerkontrolle** Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
⇨ **Speicherkontrolle** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten	⇨ **Benutzerkontrolle** Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte
⇨ **Zugriffskontrolle** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben	⇨ **Übertragungskontrolle** Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
⇨ **Pseudonymisierung und Verschlüsselung**	⇨ **Vertraulichkeit (Zugriff nur durch Befugte)** z.B.: Berechtigungskonzept, Berechtigungsvergabe nur durch vereinzelte Personen,…
⇨ **Integrität (Verlässlichkeit)** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.	⇨ **Verfügbarkeit** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
⇨ **Belastbarkeit**	⇨ **Wiederherstellbarkeit** Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.
⇨ **Überprüfung, Bewertung und Evaluierung** z.B.: regelmäßige dokumentierte Audits und Begehungen durch den DSB	⇨ **Zuverlässigkeit** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
⇨ **Eingabekontrolle** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind	⇨ **Transportkontrolle** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
⇨ **Auftragskontrolle** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können	⇨ **Trennbarkeit** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

ANLAGE 3: Information zu Bußgeldern

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften