


Argon & Co Deutschland GmbH	Informationssicherheitsmanagement	
Verpflichtungserklärung Vertraulichkeit und Informationssicherheit		

## **Verpflichtung zur Vertraulichkeit, zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) und zur Einhaltung der Informationssicherheit**


Alle Mitarbeiter der Argon & Co Deutschland GmbH verpflichten sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen:

- auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
- 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“).

Personenbezogene Daten dürfen daher nur nach Weisung des Verantwortlichen verarbeitet werden. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher.

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Argon & Co Deutschland GmbH	Informationssicherheitsmanagement	Argon&Co 
Verpflichtungserklärung Vertraulichkeit und Informationssicherheit		

**Bitte beachten Sie:**

Ihre Vertraulichkeitsverpflichtung gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kollegen, Ihrer Familie und der Presse.

Wenn Sie mit personenbezogenen Daten arbeiten, müssen Sie sich immer an die Weisungen der Geschäftsleitung halten. Sollten andere Personen oder Stellen (also beispielsweise Kunden oder Behörden) von Ihnen einen bestimmten Umgang mit oder die Herausgabe von personenbezogenen Daten verlangen, wenden Sie sich bitte immer sofort an Datenschutzbeauftragten oder die Geschäftsführung.

**Folgen der Verstöße**

Verstöße gegen das Datenschutzrecht können für die Gesellschaft schwerwiegende Folgen haben – aber auch für Sie persönlich.

Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DS-GVO). Diese Geldbuße kann bis zu € 20.000.000, - pro Verstoß betragen oder für uns als Unternehmen bis zu vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns, je nachdem, was höher ist.

Geldbußen können sogar gegen einzelne Mitarbeiter verhängt werden. Geben Sie beispielsweise ohne entsprechende Anweisung von der Gesellschaft personenbezogene Daten weiter oder nutzen Sie diese für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu € 20.000.000,- bestraft werden.

Zudem sind bestimmte Verstöße gegen das Datenschutzrecht Straftaten, die mit Gefängnis bestraft werden können (§ 42 BDSG).


Beispiel: Jemand verkauft weisungswidrig eine Festplatte mit personenbezogenen Daten, anstatt sie zu zerstören.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

Zudem kann jede betroffene Person Schadensersatz für eine unzulässige Verarbeitung ihrer Daten verlangen, und zwar einschließlich Schmerzensgeld für die Persönlichkeitsrechtsverletzung (Art. 82 DS-GVO, §§ 823 ff. BGB). Unter Umständen müssen Sie persönlich diesen Schadensersatz ganz oder teilweise bezahlen, wenn Sie mittlere oder schwere Verstöße begangen oder personenbezogene Daten weisungswidrig verarbeitet haben, z.B. wenn Sie sie für Ihre eigenen Zwecke genutzt haben.

**Fragen Sie daher lieber einmal zu viel als zu wenig.**

Nicht zuletzt können wir arbeitsrechtliche Konsequenzen ziehen, wenn Sie gegen Ihre Vertraulichkeitspflichten verstoßen. Denkbar sind je nach Schwere Ihres Fehlverhaltens ins-

Argon & Co Deutschland GmbH	Informationssicherheitsmanagement	
Verpflichtungserklärung Vertraulichkeit und Informationssicherheit		

besondere eine Abmahnung, eine fristgerechte Kündigung oder sogar eine fristlose Kündigung ohne vorherige Verwarnung.

## Verpflichtungserklärung zur Einhaltung der Informationssicherheit

Die Argon & Co Deutschland GmbH verpflichtet sich zur Einhaltung der Informationssicherheit, um den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Informationen sicherzustellen. Als Mitarbeiter der Argon & Co Deutschland GmbH verpflichte ich mich, die Standards sowie die festgelegten Richtlinien zur Informationssicherheit zu befolgen und die Sicherheit der Unternehmensdaten, Systeme und Prozesse jederzeit zu gewährleisten.

- **Vertraulichkeit:** Ich werde alle vertraulichen Informationen, die mir im Rahmen meiner Tätigkeit zur Verfügung gestellt oder zugänglich gemacht werden, schützen und nur im Rahmen meiner beruflichen Aufgaben verwenden. Unbefugte Weitergabe, Veröffentlichung oder Missbrauch von Unternehmens- oder Kundendaten ist strikt untersagt.
- **Integrität:** Ich werde alle Maßnahmen ergreifen, um die Korrektheit und Unverfälschtheit der Daten und Informationen sicherzustellen. Manipulation oder unsachgemäße Änderungen an Daten und Systemen sind untersagt.
- **Verfügbarkeit:** Ich werde sicherstellen, dass die mir anvertrauten Systeme und Daten jederzeit ordnungsgemäß verfügbar sind und ihre Funktionsfähigkeit nicht durch mein Verhalten oder unsachgemäße Handhabung gefährdet wird.
- **Einhaltung der Unternehmensrichtlinien:** Ich werde die unternehmensinternen Informationssicherheitsrichtlinien sowie alle anderen geltenden Bestimmungen und Anweisungen zum Schutz von Informationen und Systemen jederzeit beachten. Dies umfasst insbesondere die Nutzung von IT-Systemen, Passwörtern und physischen Zugängen, die Handhabung sensibler Daten und die Berichterstattung von Sicherheitsvorfällen.
- **Awareness und Schulungen:** Ich verpflichte mich, an allen notwendigen Schulungen und Sensibilisierungsmaßnahmen zur Informationssicherheit teilzunehmen und mich regelmäßig über aktuelle Bedrohungen und Schutzmaßnahmen zu informieren.
- **Meldung von Sicherheitsvorfällen:** Sollte ich einen Vorfall, Verdacht oder Verstoß gegen die Informationssicherheit bemerken, werde ich diesen unverzüglich gemäß den internen Meldeprozessen an die zuständigen Stellen weiterleiten.

Ich bin mir bewusst, dass die Missachtung dieser Verpflichtungen schwerwiegende Konsequenzen nach sich ziehen kann. Dazu gehören disziplinarische Maßnahmen wie Verwarnungen oder arbeitsrechtliche Sanktionen, bis hin zur Kündigung des Arbeitsverhältnisses. In besonders gravierenden Fällen kann dies auch rechtliche Schritte nach sich ziehen, die zivil- oder strafrechtliche Folgen haben könnten.


\_\_\_\_\_, den \_\_\_\_\_

Ort

Datum

\_\_\_\_\_  
Name Mitarbeiter:in

\_\_\_\_\_  
Unterschrift des/der Verpflichteten

Argon & Co Deutschland GmbH	Informationssicherheitsmanagement	
Verpflichtungserklärung Vertraulichkeit und Informationssicherheit		

## Anlage 1: Merkblatt zum Umgang mit personenbezogenen Daten

Bei deiner Tätigkeit für die Advyce&Company wirst du mit personenbezogenen Daten oder weiteren gesetzlich geschützten oder vertraulichen Daten in Berührung kommen. Sei es als Betroffene:r selbst, dessen personenbezogene Daten verarbeitet werden, weil du beim Umgang mit personenbezogenen Daten anderer mitwirkst oder weil dir solche Daten während deiner Tätigkeit zur Kenntnis gelangen.

### Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als natürliche Person kommen beispielsweise unsere Kunden, Lieferanten oder Beschäftigte in Betracht.

Einige Beispiele für personenbezogene Daten, sofern folgende Daten einer natürlichen Person zugeordnet werden können, sind:

Name, Vorname Anschrift (auch geschäftliche Anschrift) Gesundheitsdaten Einkommen oder Vermögen Religiöse oder philosophische Überzeugungen Geburtsdatum Telefonnummer oder E-Mail-Adresse (auch geschäftliche Kontaktdaten) Ethische oder rassische Herkunft	Familienstand Konto- oder Kreditkartennummer Biometrische oder genetische Daten Lebensalter Personalausweis oder Sozialversicherungsnummer Fotografien oder Videoaufzeichnungen Personalnummer
--	--

### Die Verarbeitung von personenbezogenen Daten

Verarbeitung meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Kurzum: jegliches „anfassen“ von personenbezogenen Daten.

erheben erfassen organisieren speichern verändern anpassen vernichten	auslesen abfragen verwenden übermitteln verknüpfen löschen verbreiten
---	---

Aufgrund der allgemeinen arbeitsvertraglichen Regelungen und gesetzlicher Vorschriften wird das Gebot zur vertraulichen Handhabung von personenbezogenen Daten sowie von Geschäftsgeheimnissen im Unternehmen bekannt gegeben. Für diejenigen Personen, welche bei der Verarbeitung personenbezogener Daten im Geltungsbereich der EU DSGVO und des BDSG beschäftigt sind, gilt darüber hinaus die gesonderte Verpflichtung auf Vertraulichkeit im Umgang mit personenbezogenen Daten.

Die Regelungen der Richtlinie zur Informationssicherheit und Datenschutz sind einzuhalten.

## **Anlage 2: Auszüge aus den einschlägigen datenschutzrechtlichen Vorschriften und gesetzlichen Regelungen**

### **Auszug aus der Europäischen Datenschutzgrundverordnung (EU DSGVO)**

#### Art. 4 Nr. 1 DSGVO Begriffsbestimmungen:

„personenbezogene Daten“ 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 DSGVO Begriffsbestimmungen:

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

#### Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

- a) 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“);
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) 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“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

#### Art. 24 DSGVO Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

#### Art. 28 DSGVO Auftragsverarbeitende

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitenden, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung 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 bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden

muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. 2Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

#### Art. 29 DSGVO Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

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 DSGVO Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) 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 unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

#### Art. 33 DSGVO Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) 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 gemäß Artikel 55 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. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

#### Art. 82 DSGVO Haftung und Recht auf Schadenersatz

(1) 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.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadensersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadensersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadensersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

#### Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

Argon & Co Deutschland GmbH – Oberanger 43, 80331 München – HRB 212105 – Geschäftsführer:  
Aurel Graf von Bassewitz, Dr. Jan Duch, Maximilian Funk, Jean-François Laget, Roland Mönikes, Andreas Offinger,  
Klaus Schug, Marc Staudenmayer, Burkhard Wagner

(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 j 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 abzuweichen 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.

Auszug aus dem Bundesdatenschutzgesetz (BDSG)

§ 42 BDSG Strafvorschriften

(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, einem Dritten übermittelt oder 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, ohne hierzu berechtigt zu sein, verarbeitet oder durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

#### § 43 BDSG Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

#### Auszug aus dem 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.


Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

#### Auszug aus dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

##### § 23 Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt, entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder

entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden

<b>Argon &amp; Co Deutschland GmbH</b>	<b>Informationssicherheitsmanagement</b>	
Verpflichtungserklärung Vertraulichkeit und Informationssicherheit		

oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer in den Fällen des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt, in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.