ARBONIA

Weisung über den Umgang mit Daten (Datenschutzweisung)

16. Juni 2020

ARBONIA

INHALTSVERZEICHNIS

ARBONIA

1 ZWECK UND ZIEL

Für die Erfüllung gesetzlicher und vertraglicher Verpflichtungen ist es unerlässlich, Personendaten zu sammeln und zu bearbeiten. Dabei sind die in den jeweiligen Ländern gültigen Datenschutzvorschriften zwingend einzuhalten. Die vorliegende Weisung zeigt auf, wie die Arbonia AG und ihre Konzerngesellschaften (nachfolgend gemeinsam "Arbonia", oder eine einzelne Konzerngesellschaft nachfolgend „Konzerngesellschaft“) mit Personendaten umgehen. Die festgehaltenen Bestimmungen geltend als Mindeststandards. Sieht das lokale Datenschutzrecht strengere Vorschriften vor, sind diese einzuhalten. Allfällige lokale Vorschriften für die Umsetzung der vorliegenden Weisung sind ebenfalls zu beachten.

Der Zweck dieser Weisung über den Umgang mit Daten („Datenschutzweisung“) ist die Feststellung, Umsetzung, der Erhalt und die ständige Verbesserung der Einhaltung des Datenschutzes, entsprechend den Anforderungen der Datenschutz-Grundverordnung der Europäischen Union 2016/679 (die **DSGVO**) und aller anderen geltenden örtlichen Datenschutzgesetze (zusammen die **anwendbaren Datenschutzgesetze**) durch Arbonia.

Die Nichteinhaltung der anwendbaren Datenschutzgesetze setzt Arbonia Risiken einer Rufschädigung und empfindlicher Geldstrafen aus (z. B. bis zu 4 % des weltweiten Umsatzes unter der DSGVO). Sie kann ausserdem unsere Kunden und Beschäftigten bestimmten Datenschutzrisiken aussetzen, wie etwa Identitätsdiebstahl oder finanziellen Verlusten. Die Einhaltung der anwendbaren Datenschutzgesetze hilft uns dabei, das Vertrauen in die Organisation von Arbonia zu erhalten und einen erfolgreichen Geschäftsbetrieb sicherzustellen.

Das Ziel dieser Datenschutzweisung ist es, den Rahmen für eine solche Einhaltung des Datenschutzes innerhalb von Arbonia bereitzustellen. Insbesondere zielt sie darauf ab, Grundprinzipien für die Verarbeitung personenbezogener Daten (die **Datenschutzgrundsätze**) umzusetzen, die in Abschnitt 6 bereitgestellt sind und für die Unternehmen der Arbonia verantwortlich sind, wenn sie als Verantwortlicher unter der DSGVO handeln, regelt die Notwendigkeit angemessener technischer und organisatorischer Massnahmen und die Meldung von Datenschutzvorfällen als Mindeststandard für alle Unternehmen von Arbonia und gilt für alle Mitarbeitenden der Arbonia sowie für die Mitglieder des Verwaltungsrates der Arbonia AG.

Weiterhin stellt sie einen Rahmen für weitere Anforderungen bereit, der für Verantwortliche und Auftragsverarbeiter unter der DSGVO (oder ähnlichen anwendbaren Datenschutzgesetzen) wie in Abschnitt 7 beschrieben gilt.

2 BEGRIFFSBESTIMMUNGEN UND DEFINITIONEN

Für den Zweck dieser Datenschutzweisung gelten die folgenden Begriffsbestimmungen und Definitionen:

Anonymisierte Daten bedeutet, dass die persönliche Identität nie durch irgendjemanden zurückverfolgt werden kann oder dass die persönliche Identität nur mit unangemessenem Zeit-, Kosten- und Arbeitsaufwand zurückverfolgt werden könnte.

Anwendbare Datenschutzgesetze steht für die Datenschutz-Grundverordnung der Europäischen Union 2016/679 (die **DSGVO**) oder alle anderen anwendbaren nationalen Datenschutzgesetze, die ähnliche Vorschriften umfassen.

Geschäftsprozesseigentümer steht für eine natürliche Person, die ein Zuständiger unter dieser Datenschutzweisung ist und für eine Verarbeitung von personenbezogenen Daten und der jeweiligen IT-Anwendung verantwortlich ist.

Einwilligung steht für die Einwilligung der betroffenen Person, also jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Verantwortlicher steht für die natürliche oder juristische Person, Behörde, Agentur oder andere Stelle, die alleine oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.

Datensicherheitszwischenfall steht für ein Ereignis, in dem ein gerechtfertigter Verdacht vorliegt, dass personenbezogene Daten unrechtmässig erfasst, gesammelt, geändert, kopiert, übermittelt und verwendet werden. Dies kann sich auf Aktionen Dritter oder von Beschäftigten beziehen.

Betroffene Person steht für eine identifizierte oder identifizierbare natürliche Person. Eine identifizierbare natürliche Person ist eine Person, 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Der **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Verzeichnis von Verarbeitungsvorgängen steht für eine Aufzeichnung über die Datenverarbeitung unter der Verantwortung des Verantwortlichen. Dieses Verzeichnis enthält sämtliche der folgenden Angaben: (i) Name und Kontaktdaten des Verantwortlichen und, wenn zutreffend, des gemeinsamen Verantwortlichen, des Vertreters des Verantwortlichen und des örtlichen Datenschutzkoordinators; (ii) die Verarbeitungszwecke; (iii) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorie personenbezogener Daten; (iv) die Kategorien der Empfänger, denen personenbezogene Daten offenbart wurden oder werden, einschliesslich Empfänger in Drittländern; (v) wenn zutreffend, Übermittlung personenbezogener Daten in ein Drittland, einschliesslich der Nennung des Drittlands und der Dokumentation geeigneter Garantien; (vi) die vorgesehenen Zeiträume für die Löschung der unterschiedlichen Kategorien personenbezogener Daten; (vii) eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmassnahmen.

Datenschutzbeauftragter oder Datenschutzkoordinator oder **DSK** steht für die in Abschnitt 5 beschriebene Person.

Personenbezogene Daten bedeutet alle Informationen (einschliesslich personenbezogener Daten besonderer Kategorien) bezüglich der betroffenen Person, daher bezüglich einer identifizierten oder identifizierbaren natürlichen Person, wie bspw. Name, Geburtsdatum, E-Mail-Adresse, Religion, Standortdaten, Online-Daten (IP-Adresse, Standortdaten, etc.), Kennnummern (Sozialversicherungsnummer, Personalausweisnummer, etc.), physische Merkmale (Geschlecht, Haut-, Haar-. Augenfarbe, etc.), Kundendaten, u.v.m.), die einer anwendbaren Datenschutzverordnung unterliegen.

Verarbeitung oder **verarbeiten** steht für 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.

Pseudonymisierung steht für die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Personenbezogene Daten besonderer Kategorien steht für Daten über die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Ansichten, strafrechtliche Verurteilungen, Gewerkschaftsmitgliedschaft, Gesundheit oder sexuelle

Orientierung der betroffenen Person oder genetische Daten, biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person.

Drittländer sind alle Nationen, die nicht ein Land der europäischen Union oder des europäischen Wirtschaftsraums oder ein Land mit einem angemessenen Datenschutzniveau, das von der EU-Kommission als angemessen betrachtet wird, sind (vgl. Liste der Länder mit angemessenem Datenschutzniveau:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Dritter steht für jeden anderen, als die betroffene Person, den Verantwortlichen oder den Auftragsverarbeiter (einschliesslich etwa Geschäftspartner, Untervertragsnehmer, Kreditauskunfteien und andere), sowie für Personen die unter der direkten Autorität des Verantwortlichen oder Auftragsverarbeiter berechtigt sind, personenbezogene Daten zu verarbeiten. Bei der Verarbeitung personenbezogener Daten unter einer Erlaubnis sind die Auftragsverarbeiter rechtlich keine Dritten unter dem Datenschutzgesetz, da sie rechtlich dem Verantwortlichen zugerechnet werden.

3 UMFANG

3.1 Organisatorischer Umfang

Diese Datenschutzweisung gilt für alle Konzerngesellschaften der Arbonia, für alle Mitarbeitenden der Arbonia und für die Mitglieder des Verwaltungsrates der Arbonia AG. Sie ist rechtsverbindlich in jeder Konzerngesellschaft umzusetzen.

3.2 Gesetze, Verordnungen, Standards und Weisungen

Diese Datenschutzweisung umfasst die Anforderungen der DSGVO und international anerkannter Datenschutzgrundsätze, ohne das bestehende nationale Recht zu ersetzen. Sie ergänzt die national anwendbaren Datenschutzgesetze. Das einschlägige nationale Recht hat bei Konflikten mit dieser Datenschutzweisung oder bei strengeren Anforderungen als diese Datenschutzweisung Vorrang. Die Inhalte dieser Datenschutzweisung müssen auch beachtet werden, wenn keine entsprechende nationale Gesetzgebung vorliegt.

Widerspricht diese Datenschutzweisung den Bestimmungen in einem bestimmten Land, so können die spezifischen Bestimmungen dieser Datenschutzweisung in Absprache mit Head Legal & Compliance in einer örtlichen Weisung übernommen werden. Die grundlegenden Inhalte und der Zweck der betroffenen Bestimmungen dürfen jedoch nicht verändert werden.

4 REGULATORISCHE GRUNDLAGE

Diese Datenschutzweisung basiert auf der DSGVO und den global akzeptierten grundlegenden Grundsätzen des Datenschutzes.

5 ROLLEN UND ZUSTÄNDIGKEITEN

- Der Geschäftsführer einer Konzerngesellschaft[1] ist zuständig dafür:
  1. letztendlich sicherzustellen, dass die jeweilige juristische Person ihre rechtlichen Verpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten erfüllt.
  2. sicherzustellen, dass die Anforderungen aus dieser Datenschutzweisung erfüllt werden (einschliesslich der Mitteilung bei Zwischenfällen im Bereich der Datensicherheit).
  3. sicherzustellen, dass das „Verzeichnis von Verarbeitungsvorgängen" auf Ebene der Konzerngesellschaft durch den Geschäftsprozesseigentümer befüllt und gepflegt wird.
  4. Einen formellen örtlichen Datenschutzbeauftragten (intern oder extern) (nachfolgend „Datenschutzbeauftragter") zu benennen, wenn dies durch die örtliche anwendbare Datenschutzverordnung verlangt wird, und diese benannte Person jährlich per Mitte Jahr Head Legal & Compliance und Internal Audit bekanntgeben.
  5. einen örtlichen Datenschutzmanager (nachfolgend „Datenschutzkoordinator") zu benennen, wenn die örtliche anwendbare Datenschutzverordnung keinen formellen örtlichen Datenschutzbeauftragten vorschreibt. Diese benannte Person ist jährlich per Mitte Jahr Head Legal & Compliance und Internal Audit bekanntzugeben.

- Der durch den Geschäftsführer einer Konzerngesellschaft bestimmte[2] örtliche Datenschutzkoordinator resp. Datenschutzbeauftragte muss:
  1. die Einhaltung dieser Datenschutzweisung und der Weisungen des Verantwortlichen oder Auftragsverarbeiters bezüglich des Schutzes personenbezogenen Daten überwachen, einschliesslich der Übertragung von Zuständigkeiten und der entsprechenden Prüfungen.
  2. den Verantwortlichen oder Auftragsverarbeiter und die Beschäftigten, die Verarbeitungspflichten unter dieser Datenschutzweisung ausführen, informieren, beraten und beaufsichtigen.
  3. auf Anfrage Ratschläge zu einer Datenschutz-Folgenabschätzung für personenbezogene Daten geben und deren Ergebnisse überwachen, sowie andere Fragen zu personenbezogene Daten beantworten, die ihm unter dieser Datenschutzweisung zugewiesen sind.

[1] Für Konzerngesellschaften, welche nicht operativ tätig sind, wird diese Zuständigkeit in Rücksprache mit Head Legal & Compliance gesondert festgelegt.
[2] Für Konzerngesellschaften, welche nicht operativ tätig sind, wird diese Zuständigkeit in Rücksprache mit Head Legal & Compliance gesondert festgelegt.

4. das „Verzeichnis von Verarbeitungsvorgängen“, welches durch die jeweilige Konzerngesellschaft geführt und durch die Geschäftsprozesseigentümer befüllt wird überwachen, aktuell halten, und jährlich per Mitte Jahr dem Geschäftsführer und Head Legal & Compliance die Vollständigkeit und die Aktualität der Liste bestätigen.
5. als Kontaktstelle des Head Legal & Compliance dienen und diese über die Verantwortung, Risiken und Probleme betreffend den Schutz personenbezogener Daten auf dem Laufenden halten.
6. Die für die IT-Anwendung zuständige IT bei der Prüfung und Genehmigung von neuen IT-Anwendungen auf Konzerngesellschaftsebene zur Verarbeitung personenbezogener Daten und jeder IT-Anwendung zur Verarbeitung besonderer Kategorien personenbezogener Daten aus Datenschutz-Sicht unterstützen.
7. die Übermittlung personenbezogener Daten in ein Drittland aus Datenschutz-Sicht genehmigen (vgl. auch nachfolgend, Ziff. 14).
8. als örtliche Anlaufstelle für die Aufsichtsbehörde zu Fragen bezüglich der Datenverarbeitung dienen, und mit der Aufsichtsbehörde zusammenarbeiten,
9. Anfragen von an der Verarbeitung personenbezogener Daten beteiligten Beschäftigten behandeln.
10. Anfragen von betroffenen Personen nach Informationen zu den personenbezogenen Daten, die Arbonia von ihnen besitzt, beantworten, oder bei einer Anfrage zu mehreren Konzerngesellschaften der Arbonia in Koordination mit Corporate IT behandeln (vgl. auch nachfolgend, Ziff. 7.4)
11. Durch den Geschäftsprozesseigentümer ausgearbeitete resp. vorgeprüfte Verträge oder Vereinbarungen mit dem Auftragsverarbeiter prüfen und genehmigen, die personenbezogene Daten im Auftrag von Arbonia wie in Abschnitt 7.2 bearbeiten können.
12. den externen örtlichen Datenschutzbeauftragten überwachen, sofern ein solcher bestellt wurde.
13. Zwischenfällen im Bereich der Datensicherheit gemäss der Data Breach Notification Weisung melden (vgl. nachfolgend Ziff. 9 sowie „Arbonia Data Breach Policy“).

- Das IT-Board gemeinsam mit Corporate IT ist zuständig dafür:
  1. die konzernweit gültigen Standards sowie generelle IT Controls (GITC), die bei der Speicherung von Daten zu beachten sind, zu definieren.

- Die jeweils zuständige IT, welche eine Konzerngesellschaft betreut ist zuständig dafür:
  1. mittels entsprechender Standards, Policies und der Durchführung der generellen IT-Kontrollen (GITC) sicherzustellen, dass Systeme, Leistungen und Ausrüstung, die zum Speichern von Daten verwendet werden, annehmbaren Sicherheitsstandards genügen (Zugriffskontrolle / Datenlöschung) wobei der Stand der Technik, die Kosten für die Umsetzung und die Art, der Umfang, Zusammenhang und der Zweck der Verarbeitung sowie die unterschiedlichen Wahrscheinlichkeiten und Schwere der Auswirkung auf die Rechte und Freiheiten natürlicher Personen zu beachten sind.

2. anzustreben, dass der Verantwortliche und der Auftragsverarbeiter angemessene technische und organisatorische Massnahmen umsetzen, um ein dem Risiko entsprechendes Schutzniveau sicherzustellen, wie in Abschnitt 8 vorgesehen.
3. nach Konsultation des Datenschutzkoordinators resp. Datenschutzbeauftragten neue IT-Anwendungen zur Verarbeitung personenbezogener Daten aus Datenschutz-Sicht prüfen und genehmigen.
4. regelmässige Prüfungen und Scans durchzuführen, um sicherzustellen, dass die Sicherheitshardware und -software korrekt funktioniert. Die Ergebnisse der Datenschutzkontrollen müssen dem zuständigen Datenschutzbeauftragten gemeldet werden.
5. die Datensicherheit aller Drittleistungen bewerten (z. B. Auftragsverarbeiter), die das Unternehmen für die Verarbeitung von personenbezogenen Daten in Betracht ziehen (beispielsweise Cloud-Computing-Leistungen, etc.)
6. Eine Liste von Zwischenfällen im Bereich der Datensicherheit zu führen, und Zwischenfälle im Bereich der Datensicherheit an Corporate IT zu melden.
7. Anfragen von betroffenen Personen nach Informationen zu personenbezogenen Daten, die die durch die jeweilige IT betreute Konzerngesellschaft der Arbonia von den betroffenen Personen besitzt, zu koordinieren und zu beantworten (vgl. auch nachfolgend Ziff. 7.4)
8. entdeckte Zwischenfällen oder Risiken im Bereich der Datensicherheit analog der Data Breach Notification Weisung melden (vgl. nachfolgend Ziff. 9 sowie „Arbonia Data Breach Policy")

- Corporate IT in Zusammenarbeit mit der für die Betreuung einer Konzerngesellschaft zuständigen IT: Ist zuständig dafür
  1. regelmässige Prüfungen und Scans durchzuführen, um sicherzustellen, dass die Sicherheitshardware und -software korrekt funktioniert. Die Ergebnisse der Datenschutzkontrollen müssen dem zuständigen Datenschutzbeauftragten gemeldet werden.
  2. Eine zentrale Liste von Zwischenfällen im Bereich der Datensicherheit zu führen.
  3. entdeckte Zwischenfällen oder Risiken im Bereich der Datensicherheit analog der Data Breach Notification Weisung melden (vgl. nachfolgend Ziff. 9 sowie „Arbonia Data Breach Policy").

- Internal Audit ist zuständig dafür:
  1. anlässlich der gemäss ordentlicher Auditplanung durchgeführten Audits im Rahmen einer risikobasierten Prüfung zu überprüfen, ob die organisatorischen Verfahren den wesentlichen Vorgaben dieser Datenschutzweisung entsprechen.

- Geschäftsprozesseigentümer ist zuständig dafür:
  1. sicherzustellen, dass der örtliche Datenschutzbeauftragte angemessen und rechtzeitig an allen Fragen beteiligt wird, die erforderlich sind, um die Verarbeitung personenbezogener Daten zu beurteilen.

2. alle Verträge oder Vereinbarungen mit dem Auftragsverarbeiter auszuarbeiten resp. vorzuprüfen, die personenbezogene Daten im Auftrag von Arbonia wie in Abschnitt 7.2 beschrieben bearbeiten können.
3. das „Verzeichnis von Verarbeitungsvorgängen", welches durch die jeweilige Konzerngesellschaft geführt wird, zu befüllen und aktuell zu halten, und jährlich per Ende April dem Datenschutzkoordinator resp. Datenschutzbeauftragte die Vollständigkeit und die Aktualität der Einträge zu bestätigen.
4. Vor Implementierung neuer Verarbeitungsvorgänge personenbezogener Daten die daraus resultierenden Risiken für die Persönlichkeit und die Grundrechte der betroffenen Person abzuschätzen, und bei voraussichtlich hohem Risiko der Verarbeitung vorab eine Datenschutz-Folgenabschätzung durchzuführen.

6 DATENSCHUTZGRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Jede Konzerngesellschaft, welche bei der Verarbeitung personenbezogener Daten als Verantwortlicher handelt, muss sicherstellen, dass es die Einhaltung der folgenden **6 (sechs) wesentlichen Datenschutzgrundsätze nachweisen kann:**

1. Nur personenbezogene Daten verarbeiten, wenn eine gültige Rechtsgrundlage unter den anwendbaren Datenschutzgesetzen nachgewiesen werden kann und die betroffene Person über die Identität und Kontaktdaten des Verantwortlichen, die Art und rechtlichen Grundlagen der erfassten personenbezogenen Daten, die jeweiligen Aufbewahrungszeiten und den Zweck informiert wird, für die die personenbezogenen Daten erfasst werden

2. Immer den Zweck beachten, für den die personenbezogenen Daten erfasst wurden

3. Nur solche personenbezogene Daten erfassen/verarbeiten, die wirklich benötigt werden

4. Personenbezogene Daten korrekt halten und unrichtige personenbezogene Daten löschen

5. Personenbezogene Daten nur für die wirklich notwendigen rechtlichen Aufbewahrungszeiträume aufbewahren

6. Personenbezogene Daten vertraulich behandeln und nur teilen, was wirklich geteilt werden muss

6.1 Fairness, Rechtmässigkeit und Transparenz

Personenbezogene Daten dürfen nur zu Zwecken verarbeiten werden, die speziell wie nachfolgend beschrieben erlaubt sind; dies muss in transparenter Weise geschehen. Daher sind personenbezogene Daten in rechtmässiger und fairer Weise zu verarbeiten und die individuellen Rechte der betroffenen Personen zu beachten. Dies kann personenbezogene Daten umfassen, die Arbonia direkt von einer betroffenen Person erhält (beispielsweise durch Ausfüllen von Formularen oder durch Korrespondenz mit uns per Post, Telefon, E-Mail oder anderweitig), sowie personenbezogene Daten, die Arbonia von Dritten erhält.

Unter den anwendbaren Datenschutzgesetzen können personenbezogene Daten rechtmässig basierend auf einem von **fünf rechtmässigen Gründen** (die **rechtmässigen Gründe**) laut der DSGVO verarbeitet werden. Diese Gründe umfassen:

1. **Vertrag:** Die Verarbeitung personenbezogener Daten ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Massnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen, oder

2. **Einwilligung:** Die Verarbeitung personenbezogener Daten basiert auf der Einwilligung (Opt-in-Modell) der betroffenen Person zu einem oder mehreren spezifischen Zwecken. Die Einwilligung muss dokumentiert sein, oder

3. **Rechtliche Verpflichtung:** Die Verarbeitung personenbezogener Daten basiert auf einer rechtlichen Verpflichtung von Arbonia. Die Art und der Umfang der Datenverarbeitung muss für die rechtlich zulässige Verarbeitungstätigkeit notwendig sein und die geltenden gesetzlichen Bedingungen einhalten, oder

4. **Öffentliches Interesse:** Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder

5. **Berechtigte Geschäftsinteressen:** Die Verarbeitung ist verhältnismässig für berechtigte Geschäftsinteressen der Arbonia oder des Dritten, an den die personenbezogenen Daten offenbart werden, ausser, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person diese Interessen überwiegen. Berechtigte Interessen sind allgemein rechtlicher (z. B. Einzug ausstehender Forderungen / durch Tarifvereinbarung mit dem Betriebsrat / Geltendmachung / Ausübung von oder Verteidigung gegen Rechtsansprüchen bezüglich der betroffenen Person) oder kommerzieller Art (z. B. vermeiden von Vertragsverletzungen).

Die Transparenz verlangt, dass die betroffene Person informiert sein muss, wie ihre personenbezogenen Daten gehandhabt werden. Allgemein wird daher empfohlen, personenbezogene Daten direkt von der betroffenen Person (und nicht über einen Dritten)

zu erfassen. Wenn die personenbezogenen Daten verarbeitet werden, muss die betroffene Person über folgendes informiert werden:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters in der EU
- gegebenenfalls die Kontaktdaten des Datenschutzkoordinators resp. Datenschutzbeauftragten
- den Zweck der Verarbeitung personenbezogener Daten sowie die Rechtsgrundlage für die Verarbeitung,
- Dritte Empfänger oder Kategorien dritter Empfänger, an die Daten übermittelt werden können
- Wenn anwendbar, Informationen zur Verarbeitung in einem Drittland und Verweis auf angemessene Garantien

6.2 Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, der der betroffenen Person vor der Erfassung der personenbezogenen Daten mitgeteilt wurde. Nachfolgende Änderungen des Zwecks sind nur zu einem beschränkten Umfang möglich und erfordern eine Begründung. Der Verantwortliche muss die betroffene Person über den Zweck informieren, zu dem Arbonia ihre personenbezogenen Daten verarbeitet, wenn Arbonia die personenbezogenen Daten erstmalig erhebt oder sobald wie möglich danach. Bei jeder Verarbeitung zu Werbezwecken oder für Marketingprogramme muss der betroffenen Person ein Widerspruchsrecht gegen die Verarbeitung ihrer personenbezogenen Daten eingeräumt werden, und sie muss ausdrücklich über dieses informiert werden. Insofern muss jeder Verantwortliche eine Verarbeitung von Beschwerden umsetzen, die sicherstellt, dass Opt-Outs respektiert werden.

6.3 Datenminimierung

Nur solche personenbezogene Daten verarbeiten, die wirklich benötigt werden. Vor der Verarbeitung personenbezogener Daten muss festgestellt werden, ob und zu welchem Umfang die Verarbeitung personenbezogener Daten notwendig ist, um den Zweck zu erreichen, für den sie erfolgt. Personenbezogene Daten dürfen nicht im Voraus erfasst und für potenzielle künftige Zwecke gespeichert werden, sofern dies nicht durch nationales Recht verlangt oder erlaubt wird.

6.4 Richtig und aktuell

Personenbezogene Daten müssen richtig, vollständig und - wenn Änderungen auftreten - aktuell gehalten werden. Es sind geeignete Schritte zu ergreifen, um sicherzustellen, dass unrichtige oder unvollständige personenbezogene Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden. Alle, die mit personenbezogenen Daten arbeiten, müssen jeweils angemessene Schritte hierfür ergreifen (beispielsweise durch Bestätigung der Daten einer betroffenen Person, wenn diese anruft, oder die Entfernung einer gespeicherten

Telefonnummer aus der Datenbank, wenn die betroffene Person diese nicht mehr verwendet).

6.5 Beschränkte Aufbewahrungsdauer

Personenbezogene Daten dürfen nur für die wirklich benötigte Speicherdauer aufbewahrt werden. Personenbezogene Daten müssen gelöscht werden, sobald sie nicht mehr für die vorgesehenen Zwecke erforderlich sind oder die Einwilligung widerrufen oder der Verwendung auf Grundlage eines berechtigten Interesses widersprochen wird, und Arbonia keine vorrangigen berechtigten Gründe anführen kann. In einigen Fällen können längere Speicherzeiträume uns erlauben, personenbezogene Daten länger aufbewahren, wenn dies gesetzlich verlangt wird (z. B. unter Steuer- und Handelsgesetzen), oder personenbezogene Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind.

6.6 Vertraulichkeit und Datensicherheit

Personenbezogene Daten sind jederzeit vertraulich zu behandeln und nur so zu teilen, wie sie wirklich geteilt werden müssen. Der Grundsatz der "benötigten Information" gilt, sodass Beschäftigte und Dritte nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für die Erfüllung des Zwecks notwendig ist. Dies verlangt ein sorgfältig erstelltes Konzept, das die spezifischen Zugriffsrechte für jeden Geschäftsablauf definiert, einschliesslich der Umsetzung und Genehmigung der Rollen und Zuständigkeiten (Konzept des Zugangsrechts). Empfänger personenbezogener Daten sind über die Vertraulichkeit der personenbezogenen Daten zu informieren **und müssen sich einer Geheimhaltungsvereinbarung/Vertraulichkeitsvereinbarung unterwerfen** (die Teil des Arbeitsvertrags oder ähnliches sein kann). Ausnahme: Der Empfänger unterliegt einer beruflichen oder gesetzlichen Geheimhaltungspflicht.

Personenbezogene Daten sind mit geeigneten organisatorischen und technischen Massnahmen zu sichern, um unrechtmässigen Zugang, unrechtmässige Verarbeitung oder Offenbarung sowie unbeabsichtigten Verlust, Änderung oder Vernichtung zu verhindern (vgl. Abschnitt 8).

7 WEITERE PFLICHTEN UNTER DER DSGVO ODER ANDEREN ÄHNLICHEN ANWENDBAREN DATENSCHUTZVERORDNUNGEN

7.1 Grundsatz der Rechenschaftspflicht

Eine Konzerngesellschaft der Arbonia, welche der DSGVO (oder einer ähnlichen anwendbaren Datenschutzverordnung) unterliegt, muss sicherstellen, dass es die Einhaltung der anwendbaren Datenschutzgesetze nachweisen kann (der Grundsatz der "Rechenschaftspflicht"). Daher müssen diese Konzerngesellschaften neben den allgemeinen Anforderungen unter dieser Datenschutzweisung folgende Punkte umsetzen und

aufrechterhalten, wobei der Geschäftsführer der entsprechenden Konzerngesellschaft letztendlich die Umsetzung und Aufrechterhaltung sicherzustellen hat:

1. Örtlicher Datenschutzkoordinator resp. örtlicher Datenschutzbeauftragte: Benennen eines speziellen örtlichen Datenschutzkoordinators bzw. Datenschutzbeauftragten

2. Führung des „Verzeichnis von Verarbeitungsvorgängen": Es ist ein Inventar über die Verarbeitungsaktivitäten personenbezogener Daten zu führen und aktuell zu halten

3. Legitimationsprüfung: Die rechtmässige Verarbeitung personenbezogener Daten unter Einhaltung der gültigen rechtmässigen Gründe ist zu prüfen, vor allem bei der Verarbeitung von besonderen Kategorien personenbezogener Daten

4. Kontrolle des Auftragsverarbeiters: Abschliessen eines Auftragsverarbeitungsvertrags mit dem Auftragsverarbeiter oder als Auftragsverarbeiter bei der Erbringung oder dem Empfang personenbezogener Daten unter einer Erlaubnis nach Art. 28 DSGVO.

5. Bei gemeinsam für die Verarbeitung Verantwortlichen ist eine Vereinbarung zwischen den gemeinsam für die Verarbeitung Verantwortlichen nach Art. 26 DSGVO vorzusehen.

6. Beschäftigte der Arbonia sind über die Verarbeitungstätigkeit zu personenbezogenen Daten zu informieren.

7.2 Regeln für den Auftragsverarbeiter (vor allem Dienstleistungspartner)

Der Verantwortliche arbeitet nur mit Auftragsverarbeitern zusammen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so ergriffen werden, dass die Verarbeitung personenbezogener Daten im Einklang mit den Anforderungen von Artikel 28 DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Für geteilte Leistungen innerhalb von Arbonia liegt eine Vereinbarung vor, die es gestattet, personenbezogene Daten zu übermitteln, sofern rechtmässige rechtliche Gründe für die Übermittlung dieser personenbezogenen Daten nach den anwendbaren Datenschutzgesetzen vorliegen.

7.2.1 Bereitstellen personenbezogener Daten an den Auftragsverarbeiter (ausgehend)

Die Verarbeitung personenbezogener Daten unter einer Erlaubnis bedeutet, dass ein Dienstleister beauftragt wird, personenbezogene Daten zu verarbeiten, ohne die Verantwortung für das entsprechende Geschäftsverfahren übertragen zu bekommen (d. h. Dienstleister, Outsourcing-Leistungen). In diesem Fall ist ein Auftragsverarbeitungsvertrag für die Verarbeitung personenbezogener Daten unter einer Erlaubnis mit externen Anbietern zu schliessen. Die jeweilige Konzerngesellschaft der Arbonia ist der Verantwortliche und behält die vollständige Verantwortung für die korrekte Ausführung der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter.

Der jeweilige Geschäftsprozesseigentümer muss sicherstellen, dass die aktuelle Modellvereinbarung für die Auftragsverarbeitung, oder ein entsprechender ähnlicher Vertrag, der durch den Dienstleister bereitgestellt wird, um die Anforderungen aus Artikel 28 DSGVO zu erfüllen, verwendet wird, um solche Dienstleister zu beauftragen. Alternativ kann ein Dienstleister seine Einhaltung der Datensicherheitsanforderungen dokumentieren, indem er eine geeignete und genehmigte EU-Zertifizierung vorlegt. Jede Abweichung von einem solchen Sicherheitsstandard muss durch den Datenschutzbeauftragten resp. den Datenschutzkoordinator in Zusammenarbeit mit Corporate IT genehmigt werden. Bestehende Verträge müssen innerhalb eines Jahres nach dem Inkrafttreten dieser Datenschutzweisung überarbeitet werden und einen schriftlichen Auftragsverarbeitungsvertag enthalten.

7.2.2 Empfangen personenbezogener Daten als Auftragsverarbeiter (eingehend)

Wenn personenbezogene Daten durch einen Dritten an eine Arbonia Konzerngesellschaft übertragen werden, muss sichergestellt werden, dass die personenbezogenen Daten (i) für den vorgesehenen Zweck verwendet werden können, (ii) basierend auf rechtmässigen Gründen erhoben werden (es wird empfohlen, eine schriftliche Bestätigung einzuholen) und (iii) ein Auftragsverarbeitungsvertrag, der Artikel 28 DSGVO entspricht, vorliegt.

7.3 Grenzüberschreitende Übermittlung personenbezogener Daten

Bei grenzüberschreitender Übermittlung personenbezogener Daten müssen die jeweiligen nationalen Anforderungen für die Offenbarung personenbezogener Daten ins Ausland erfüllt sein. Unter der DSGVO darf eine Übermittlung personenbezogener Daten innerhalb der EU, dem EWR oder in ein Land, von dem die Europäische Kommission festgestellt hat, dass das Land angemessene Garantien erfüllt, um ein angemessenes Datenschutzniveau sicherzustellen, stattfinden. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung. Die Europäische Kommission hat u.A. die Schweiz als angemessenen Schutz bietend eingestuft (vgl. aktuelle Länderliste:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Eine Übermittlung personenbezogener Daten an ein Drittland ist nur zulässig, wenn weitere angemessene Garantien vorliegen. Dies bedeutet, wenn der Empfänger nachweisen kann, dass er einen Datenschutzstandard unterhält, der dieser Datenschutzweisung entspricht (z.B. i) verbindliche Unternehmensregeln vorliegen, ii) EU-Standardvertragsklauseln für Auftragsverarbeitung in Drittländern mit dem Dienstleister und anderen Untervertragsnehmern geschlossen wurden[3], iii) durch die Aufsichtsbehörde genehmigte Verhaltensregeln vorhanden sind, iv) bei Beteiligung des Dienstleisters an einem Zertifizierungssystem, das durch die EU akkreditiert wurde, für die Erreichung eines ausreichenden Datenschutzniveaus oder v) mit einzelnen Vereinbarungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter unter der Erlaubnis der zuständigen Aufsichtsbehörde) und mit Information der betroffenen Person. Diese Pflicht gilt nicht, wenn die Übermittlung auf einer rechtlichen Verpflichtung basiert. Eine solche Übermittlung erfordert die Genehmigung durch den Datenschutzkoordinator resp. Datenschutzbeauftragten.

Wenn personenbezogene Daten innerhalb von Arbonia übermittelt werden, ist die Konzerngesellschaft, das die personenbezogenen Daten importiert, verpflichtet, mit allen Anfragen zu kooperieren, die durch die zuständige Aufsichtsbehörde in dem Land gestellt werden, in dem die exportierende Konzerngesellschaft seinen eingetragenen Sitz hat, und allen Anmerkungen zu entsprechen, die die jeweilige Aufsichtsbehörde bezüglich der Verarbeitung der übermittelten personenbezogenen Daten macht.

7.4 Umgang mit einer Informationsanfrage durch eine betroffene Person

Betroffene Personen haben das Recht, eine formelle Anfrage zu Informationen über die Details der personenbezogenen Daten zu stellen, die Arbonia besitzt und können folgendes verlangen:

Auskunftsrecht über:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch offen gelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

[3] Vgl. Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden;
- das Bestehen einer automatisierten Entscheidungsfindung, einschliesslich Profiling;
- Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien unterrichtet zu werden.

Recht auf Berichtigung:

- Die betroffene Person hat das Recht, von dem Verantwortlichen 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.

Recht auf Löschung („Recht auf Vergessenwerden"):

- Die betroffene Person hat das Recht, von dem Verantwortlichen 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:
    1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;
    2. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäss Artikel 6 Absatz 1 Buchstabe a DSGVO oder Artikel 9 Absatz 2 Buchstabe a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
    3. Die betroffene Person legt gemäss Artikel 21 Absatz 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäss Art. 21 Absatz 2 DSGVO Widerspruch gegen die Verarbeitung ein;
    4. Die personenbezogenen Daten wurden unrechtmässig verarbeitet;
    5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Recht der jeweiligen Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt;
    6. Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäss Artikel 8 Absatz 1 DSGVO erhoben.

Recht auf Einschränkung der Verarbeitung:

- Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- wenn die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen:
- wenn die Verarbeitung unrechtmässig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
- wenn der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt,
- wenn die betroffene Person Widerspruch gegen die Verarbeitung gemäss Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Die betroffene Person sollte gebeten werden, ihre Anfrage schriftlich zu stellen, entweder per E-Mail oder per Post, und adressiert an den jeweiligen örtlichen Datenschutzbeauftragten. Informationen sind der betroffenen Person durch den örtlichen Datenschutzbeauftragten unverzüglich zur Verfügung zu stellen, aber in jedem Fall innerhalb eines Monats nach Eingang der Anfrage. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Datenschutzkoordinator oder Datenschutzbeauftragte des Verantwortlichen unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Der betroffenen Person dürfen keine Kosten für die Anforderung von Auskunft über die Informationen, die eine Konzerngesellschaft der Arbonia über sie besitzt, entstehen, sofern Anfragen einer betroffenen Person nicht offensichtlich unbegründet oder exzessiv sind, insbesondere aufgrund der wiederholten Stellung. Anfragen einer betroffenen Person zu mehreren Konzerngesellschaften der Arbonia sind zur Koordination und für eine Antwort an Corporate IT weiterzuleiten.

7.5 Durchführung einer Datenschutz-Folgenabschätzung

Hat eine geplante, neue Form der Verarbeitung personenbezogener Daten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge, ist vorgängig eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Vor Implementierung neuer Verarbeitungsvorgängen sind daher die daraus resultierenden Risiken für die Persönlichkeit und die Grundrechte der betroffenen Person abzuschätzen. Bei neuen IT-Anwendungen ist dies im Rahmen des Genehmigungsablaufs zu berücksichtigen. Ist aufgrund einer ersten Abschätzung darauf zu schliessen, dass eine geplante, neue Form der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die betroffene Person zur Folge hat, ist eine Datenschutz-Folgenabschätzung durchzuführen.

Anfragen zur Notwendigkeit resp. während der Durchführung einer Datenschutz-Folgenabschätzung sind an den örtlichen Datenschutzkoordinator resp. örtlichen Datenschutzbeauftragten zu richten. Nach Durchführung ist die Datenschutz-Folgenabschätzung dem örtlichen Datenschutzkoordinator resp. örtlichen Datenschutzbeauftragten bekanntzugeben, und von diesem eine Stellungnahme einzuholen.

Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko für die betroffene Person zur Folge hätte, und werden keine Massnahmen zur Eindämmung des Risikos getroffen, so ist vor der Implementierung der neuen Verarbeitungsvorgänge die Aufsichtsbehörde zu konsultieren.

8 SICHERHEIT PERSONENBEZOGENER DATEN

Personenbezogene Daten müssen vor unrechtmässigem Zugang und unrechtmässiger Verarbeitung oder Offenbarung sowie gegen unbeabsichtigten Verlust, Änderung oder Vernichtung geschützt werden. Dies gilt unabhängig davon, ob personenbezogene Daten elektronisch oder auf Papier verarbeitet werden.

Verantwortliche und Auftragsverarbeiter müssen angemessene technische und organisatorische Massnahmen umsetzen, um Daten vor unrechtmässiger Verarbeitung zu schützen. Diese Massnahmen müssen basieren auf (i) besten Verfahren, (ii) den Risiken der Verarbeitung und (iii) der Notwendigkeit, die personenbezogenen Daten zu schützen (bestimmt durch den Ablauf für die Klassifizierung von Informationen); sie umfassen unter anderem, wie jeweils angemessen:

(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.

Die technischen und organisatorischen Massnahmen für den Schutz personenbezogener Daten sind Teil des internen Informationssicherheitsmanagements und müssen ständig an die technischen Entwicklungen und organisatorischen Änderungen angepasst werden.

Sicherheitsverfahren können mindestens umfassen:

- Zutrittskontrollen: Jeder Fremde, der in zutrittskontrollierten Bereichen vorgefunden wird, sollte gemeldet werden.

- Sichere absperrbare Schubladen oder Aktenschränke: Schreibtisch und Schränke sollten abgesperrt bleiben, wenn sie vertrauliche Informationen irgendeiner Art enthalten. Personenbezogen Daten sind immer vertrauliche Informationen. Beschäftigte sollten sicherstellen, dass Papier und Ausdrucke mit personenbezogenen Daten nicht allgemein sichtbar hinterlassen werden, wie etwa in einem Drucker. Sofern personenbezogene Daten mit Berechtigung auf einem Datenwechselträger (wie einer CD, einem Speicherstick oder einer DVD) gespeichert werden, ist dieser sicher weggesperrt aufzubewahren, wenn er nicht in Verwendung ist.
- Entsorgungsmethoden: Dokumente auf Papier sollten geschreddert und sicher entsorgt werden, wenn sie nicht mehr benötigt werden. Dies gilt auch für personenbezogene Daten, die üblicherweise elektronisch gespeichert sind, die jedoch ausgedruckt wurden.

- In elektronischer Form gespeicherte Daten: Personenbezogene Daten sollten durch Passwörter der aktuellen Passwortrichtlinie entsprechend geschützt und nie unter den Beschäftigten geteilt werden. Wenn elektronische Form zutreffend, müssen personenbezogene Daten auf IT-Server-Systemen und in strukturierten Informationstechnologieanwendungen gespeichert und abgerufen werden, statt unverschlüsselt auf lokalen Computern.

- In elektronischer Form erhobene personenbezogene Daten, die durch die betroffene Person bereitgestellt wurden: Die Identität der betroffenen Person ist zu überprüfen, vorzugsweise durch einen doppelten Opt-In-Prozess bestimmt (also eine zweite E-Mail zur Validierung der angegebenen E-Mail-Adresse). Wenn Zugang zu einer Website oder App auf registrierte Benutzer eingeschränkt wird (d. h. Benutzerkonto), muss die Identifizierung und Authentifizierung der betroffenen Person einen Sicherheitsschutz bieten, der während des Zugriffs proportional zu den jeweiligen Inhalten ist.

- Ausübung von Vorsicht beim Teilen personenbezogener Daten: Personenbezogene Daten sollten nie informell geteilt werden. Der Grundsatz der "notwendigen Informationen" gilt. Ein Konzept der Aufschlüsselung und Trennung pro Geschäftsablauf sowie der Umsetzung von Rollen und Zuständigkeiten ist verpflichtend. Personenbezogene Daten sind vor der Übermittlung in elektronischer Form zu verschlüsseln. Der Informationstechnologiemanager kann erklären, wie personenbezogene Daten an autorisierte externe Kontaktpersonen verschickt werden.

- Anleitung einholen: Bei Fragen oder Unsicherheit betreffend eines Aspekts des Datenschutzes oder betreffend Pflichten aus dieser Datenschutzweisung ist Rat zu suchen beim direkten Vorgesetzten, dem jeweiligen örtlichen Datenschutzbeauftragten oder bei Legal & Compliance.

Die DSGVO verlangt, dass die Privatsphäre so frühzeitig wie möglich in Betracht gezogen wird. Die Privatsphäre durch Technikgestaltung verlangt, dass Organisationen die Privatsphäre in den ersten Stufen der Technikgestaltung und während es gesamten Entwicklungsablauts neuer Produkte, Verfahren oder Dienstleistungen, die mit der Verarbeitung personenbezogener Daten zu tun haben, in Betracht ziehen. Privatsphäre durch Voreinstellung bedeutet, dass, wenn ein System oder ein Dienst die Entscheidung des Einzelnen umfasst, wie viele personenbezogene Daten er mit anderen teilt, die Voreinstellungen diejenigen sein sollten, die den grössten Schutz für die Privatsphäre bieten. Daher unterliegt jede neue IT-Anwendung einem internen Genehmigungsablauf, wobei diese neue IT-Anwendung im Rahmen der Evaluierung auch unter datenschutzrechtlichen Gesichtspunkten zu evaluieren ist.

9 MELDUNG VON ZWISCHENFÄLLEN IM BEREICH DER DATENSICHERHEIT

Viele anwendbare Datenschutzverordnungen verlangen eine direkte Meldung von Zwischenfällen im Bereich des Datenschutzes an den Gesetzgeber. Daher wird verlangt, dass alle Zwischenfälle im Bereich der Datensicherheit umgehend an den zuständigen Datenschutzkoordinator oder Datenschutzbeauftragten gemeldet werden, unabhängig davon, ob ein örtliches System oder ein Konzernsystem betroffen ist, entsprechend dem Ablauf, der in der Weisung von Arbonia zu Zwischenfällen im Bereich der Datensicherheit beschrieben ist („Arbonia Data Breach Policy"). Stellt die IT Zwischenfälle oder Risiken im Bereich der Datensicherheit fest, sind diese analog der Data Breach Notification Weisung zu melden.

Das Ziel ist die Einhaltung der Pflichten über die Meldung einer Verletzung geltender Datenschutz Verpflichtungen unter den anwendbaren Datenschutzgesetzen (z. B. unter der DSGVO spätestes innerhalb von 72 Stunden nach Kenntnisnahme).

In einem solchen Fall muss die Betonung darauf liegen, die jeweiligen Deadlines für die Benachrichtigung über Verletzungen des Datenschutzes einzuhalten und umgehend Massnahmen zu ergreifen, um Zwischenfälle zu untersuchen und festzustellen, ob personenbezogene Daten tatsächlich verletzt wurden. Corporate IT muss ein internes Verzeichnis von Sicherheitsverletzungen bei Arbonia führen, sodass Meldepflichten unter dem nationalen Recht eingehalten werden können und sicherstellen, dass die jeweilige Vertretungsregeln angewendet werden, um Verletzungen jederzeit melden zu können. Vor der Meldung an eine nationale Behörde ist Corporate IT oder die Abteilung Legal and Compliance des Konzerns zu informieren.

ARBONIA

Alle weiteren Weisungen der Corporate IT sowie der lokalen IT-Abteilungen sind strikte einzuhalten.

10 FOLGEN BEI NICHTEINHALTUNG

Die Einhaltung dieser Datenschutzweisung ist von äusserster Wichtigkeit für Arbonia und die öffentliche Wahrnehmung der Arbonia. Unangemessene Verarbeitung personenbezogener Daten oder andere Verletzungen der Datenschutzgesetze kann in vielen Ländern auch einer strafrechtlichen Verfügung unterliegen und zu Ansprüchen auf Schadensersatz führen. Innerhalb von Arbonia kann eine Verletzung der Regeln aus dieser Datenschutzweisung Sanktionen unter dem Gesetz und/oder dem jeweiligen (Arbeits-)Vertrag nach sich ziehen.

11 ABWEICHUNGEN

Abweichungen von den Bestimmungen dieser Weisung und der Zusätze sind nur nach Rücksprache mit dem Head of Legal & Compliance zulässig.

12 AUSKÜNFTE

Auskünfte im Zusammenhang mit der Datenschutzweisung erteilt der Head of Legal & Compliance.

13 INKRAFTTRETEN

Diese Weisung tritt per 17. Juni 2020 in Kraft und ersetzt die Weisung über den Umgang mit Daten (Datenschutzweisung) vom 5. Dezember 2013.

Arbon, 16. Juni 2020

Arbonia AG

Alexander von Witzleben
Präsident des Verwaltungsrats und CEO

Andrea Wickart
Head Legal & Compliance / Generalsekretärin

ARBONIA

Zusätze zu dieser Arbonia Datenschutzweisung:

Die folgenden Zusätze in Ihrer aktuellen Fassung konkretisieren diese Datenschutzweisung:

- Weisung zu Anträgen betroffener Personen und zur Löschung von Daten
- Weisung zu Datenschutzverletzungen
- Datenschutzerklärung für Mitarbeitende

Dieses Dokument ist ohne Unterschrift gültig.