



xPlan
Pensionskassensoftware

Umsetzung des neuen Datenschutzgesetzes für Pensionskassen

Inhaltsverzeichnis

Handlungsbedarf für Ihre Pensionskasse

- Wichtigste Datenschutzfragen im Vorsorgebereich
 - Zuordnung als Bundesorgan oder Private
 - Einordnung als Verantwortlicher oder Auftragsbearbeiter
 - Geschäftsführung der Stiftung
 - Einsetzung eines Datenschutzberaters (Aufgaben)
 - Datenschutz-Folgenabschätzung
 - Information bei der Datenbeschaffung
 - Betroffenenrechte
 - Erstellung von Verzeichnissen und weiteren Dokumentationen
- Beispiel Umsetzung aXenta



Handlungsbedarf für Ihre Pensionskasse

Zuordnung als Bundesorgan oder Private

- Das nDSG gilt für Bundesorgane und Private
- Pensionskassen bzw. Vorsorgestiftungen gelten als Bundesorgane, wenn sie (ganz oder teilweise) im obligatorischen Bereich tätig sind.



Handlungsbedarf für Ihre Pensionskasse

Verantwortlicher oder Auftragsbearbeiter

- Das nDSG kennt bei der Bearbeitung von Personendaten zwei Rollen:
 - Ein **Verantwortlicher** bestimmt den Zweck und die Mittel einer Datenbearbeitung, er veranlasst diese.
 - Ein **Auftragsbearbeiter** bearbeitet Personendaten im Auftrag und für die Zwecke des Verantwortlichen.
- Aus der Rollenverteilung konkretisieren sich die datenschutzrechtlichen Pflichten und Zuständigkeiten der jeweiligen Akteure.



Handlungsbedarf für Ihre Pensionskasse

Geschäftsführung der Stiftung

- Das Kleid der Pensionskasse, sprich ob es sich zum Beispiel um eine firmeneigene Stiftung, eine Sammelstiftung oder eine Bankstiftung handelt, ist von Bedeutung.
- Daraus leitet sich das datenschutzrechtliche Verhältnis zum Arbeitgeber, zum Arbeitnehmer/Vorsorgenehmer und gegebenenfalls weiteren Begünstigten ab. Dies ist im Vorsorgereglement und gegebenenfalls in weiteren Dokumenten abzubilden.
- Zunehmend relevant wird mittelbar auch die Frage nach der Rolle der Broker.



Handlungsbedarf für Ihre Pensionskasse

Einsetzung eines Datenschutzberaters

- **Bundesorgane müssen einen Datenschutzberaten benennen** und diesen dem Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden.
- Dieser ist einerseits organisatorisch so einzubinden, dass er über sämtliche Vorgänge Bescheid weiss, zugleich aber **weisungsungebunden agieren** kann.
- Findet sich intern keine geeignete Person, kann auch ein externer Datenschutzberater bestellt werden.



Handlungsbedarf für Ihre Pensionskasse

Datenschutz-Folgenabschätzung

- Diese Selbstbeurteilung in Bezug auf bestimmte Datenbearbeitungen ist erforderlich, wenn eine Datenbearbeitung an sich hohe Risiken für die betroffenen Personen mit sich bringt.
- Können diese Risiken, trotz aller implementierten Massnahmen nicht eliminiert werden, ist der EDÖB zu konsultieren.



Handlungsbedarf für Ihre Pensionskasse

Information bei der Datenbeschaffung

- Betroffene sind bei der Beschaffung der Personendaten über die Datenbearbeitungsvorgänge zu informieren. Datenschutzerklärungen (DSE) werden unter dem nDSG daher (faktisch) zur Pflicht.
- Für Bundesorgane besteht ferner eine Pflicht, Datenempfänger über Richtigkeit, Vollständigkeit und Aktualität der gelieferten Daten zu informieren, sofern sich diese Informationen nicht bereits aus den Umständen ergeben.



Handlungsbedarf für Ihre Pensionskasse

Betroffenenrechte

- Bei den Betroffenenrechten handelt es sich um die Rechte der Personen über ihre Personendaten. Praxisrelevant sind insbesondere Auskunfts-, Berichtigungs- und Lösungsbegehren.
- Es gelten gesetzliche Voraussetzungen und Ausnahmen für Pensionskassen, die Personendaten trotz Widerspruchs weiterhin bearbeiten, um ihre gesetzlichen und vertraglichen Pflichten zu erfüllen.
- Es ist zu prüfen, ob den gesetzlichen Voraussetzungen für die Betroffenenanfragen zu entsprechen ist oder aber ob gesetzliche Ausnahmen die Pensionskasse berechtigen oder **sogar verpflichten, die Betroffenenanfrage abzulehnen.**



Handlungsbedarf für Ihre Pensionskasse

Erstellung von Verzeichnissen und weiteren Dokumentationen

- Jede bearbeitende Stelle muss ein Verzeichnis mit einem Mindestinhalt von Informationen zu vorgenommenen Datenbearbeitungen erstellen und unterhalten.
- Pensionskassen bearbeiten in grossem Umfang besonders schützenswerte Personendaten.
- Pensionskassen müssen Bearbeitungsreglemente mit weiteren Angaben zur internen Organisation, zum Datenbearbeitungsgrund, zu Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit erstellen.



Handlungsbedarf für Ihre Pensionskasse

Beispiel Umsetzung bei aXenta



Applikationsverzeichnis

Verfügen Sie über ein vollständiges Verzeichnis der in der Organisation eingesetzten Applikationen?

- Das Anwendungsverzeichnis dient als Ausgangspunkt für die Umsetzung.
- Wir prüfen und erfassen:
 - die nDSG Relevanz
 - den Zweck ihrer eingesetzten Applikationen
 - unter welcher Kategorie die Daten fallen
 - wer die Benutzer sind
 - die Betriebsplattform
 - den aktuellen Status im Lebenszyklus



Bespiel Applikationsverzeichnis

revDSG relevant?	Name	Beschreibung	Kategorie	User Base	Standard- / Individual- Lösung	Betriebsplattform	Lifecycle Status	Anmerkungen
[Ja/Nein]	[Freitext]	[Freitext]	[Freitext]	[Freitext]	[Freitext]	[Freitext]	[Freitext]	[Freitext]
Ist diese Applikation Teil einer Bearbeitung von Personendaten im Sinne des DSG?	Name der Applikation	Welchem Zweck dient diese Applikation?		Wer nutzt diese Applikation?				Anmerkungen (optional)
revDSG relevant?	Name2	Beschreibung	Kategorie	User Base	Standard- / Individual- Lösung	Betriebsplattform	Lifecycle Status	Anmerkungen
Ja	Infoniga ONE 50	Die Lohnbuchhaltung oder auch Lohnbuchführung beschäftigt sich mit Finanzen		Interne Mitarbeiter: Standard		Cloud	Live	
Ja	MediaWiki	Intranet Software, Telefonliste mit persönlichen Mobiltelefonnummern für Notfälle	Allgemein	Interne Mitarbeiter: Standard		Lokal ("On Premise")	Live	
Ja	projekto.pro - Zeit AG	Projektzeiterfassung für die Mitarbeiter	HR	Interne Mitarbeiter: Standard		Lokal ("On Premise")	Live	
Ja	presento.pro - Zeit AG	Präsenzeiten der Mitarbeiter erfassen, Stammdaten	HR	Interne Mitarbeiter: Standard		Lokal ("On Premise")	Live	
Ja	Microsoft 365	Office Software für die Mitarbeiter, Software für unsere Telefonie, E-Mail und Chat Kommunikation	Allgemein	Interne Mitarbeiter: Standard		Cloud	Live	Rechenzentrum Microsoft Zürich
Ja	Swiss Quality Broker Internatio	Meldung von Bagatellunfallmeldung, Krankentaggeld- / Geburtenmeldung, Unfallmeldung	HR	Interne Mitarbeiter: Standard		Cloud	Live	
Ja	JC Clavarex	Biometrische Authentifizierung zu den Büros des aXenta	Allgemein	Interne Mitarbeiter: Standard		Lokal ("On Premise")	Live	
Ja	Bexio	Adressverwaltung	Kundinnen	Interne Mitarbeiter: Standard		Cloud	Live	

Verzeichnis Bearbeitungstätigkeiten

Verfügen Sie über ein vollständiges Verzeichnis der Bearbeitungen von Personendaten in Ihrer Organisation?

- Wir erfassen jede Bearbeitungstätigkeit, die Sie im Auftrag eines Verantwortlichen als Auftragsbearbeiter durchführen.
- Hinzu kommen die technischen und organisatorischen Massnahmen.
- Wir verfügen über eine umfangreiche Sammlung an Frameworks, welche Sie bei der Definition von Massnahmen unterstützen.

Beispiel Bearbeitungstätigkeiten

Geschäftsprozess	Applikation(en)	1. Auftragsbearbeitung		2. Prozessdurchführung					3. Bearbeitung im Zustand				
		1.1 Auftragsbearbeitung?	1.2 Auftragsanmeldung, -Vorbereitung	2.1 Prozessverantwortliche Person	2.2 Bearbeitungsbedingung	2.3 Ereignis/Anlass	2.4 Kategorien betroffener Personen	2.5 Kategorien betroffener Prozessinstanzen	2.6 Kategorien von Bearbeitern und Empfänger	2.7 Schlüsselwörter	2.8 Technische und organisatorische Maßnahmen	3.1 Kennzeichen im Zustand	3.2 Zustandsübergang
Bearbeitung Geschäftsprozess	Applikation(en)	Ja/Nein	Inhaltsaufzeichnung (z.B. Formular)	Name, Name (off. Abkürzung)	z.B. Abgang von Geschäftsbedingungen, Rechtsantragstellung, Kündigung, etc.	z.B. Abgang von Geschäftsbedingungen, Rechtsantragstellung, Kündigung, etc.				Abgang von Geschäftsbedingungen, Rechtsantragstellung, Kündigung, etc.			
Verwaltungsgeschäft	Verwaltungsgeschäft	Ja		Verwaltungsgeschäft	Verwaltungsgeschäft	Verwaltungsgeschäft	Verwaltungsgeschäft	Verwaltungsgeschäft	Verwaltungsgeschäft	Verwaltungsgeschäft			
Personaldienstleistungen	Personaldienstleistungen	Ja		Personaldienstleistungen	Personaldienstleistungen	Personaldienstleistungen	Personaldienstleistungen	Personaldienstleistungen	Personaldienstleistungen	Personaldienstleistungen			
Arbeitsvermittlung	Arbeitsvermittlung	Ja		Arbeitsvermittlung	Arbeitsvermittlung	Arbeitsvermittlung	Arbeitsvermittlung	Arbeitsvermittlung	Arbeitsvermittlung	Arbeitsvermittlung			
Wahlrecht, Abstammung	Wahlrecht, Abstammung	Ja		Wahlrecht, Abstammung	Wahlrecht, Abstammung	Wahlrecht, Abstammung	Wahlrecht, Abstammung	Wahlrecht, Abstammung	Wahlrecht, Abstammung	Wahlrecht, Abstammung			
Abrechnung & Dokumentation	Abrechnung & Dokumentation	Ja		Abrechnung & Dokumentation	Abrechnung & Dokumentation	Abrechnung & Dokumentation	Abrechnung & Dokumentation	Abrechnung & Dokumentation	Abrechnung & Dokumentation	Abrechnung & Dokumentation			

Datenschutzerklärungen

Entspricht Ihre Datenschutzerklärung den aktuellen gesetzlichen Anforderungen?

- Umfassende Datenschutzerklärung für die Publikation auf Ihrer Webseite:
 - Wir berücksichtigen Inhalt Ihrer externen Lieferanten
 - Versenden sie Newsletter, und falls ja, mit oder ohne Analyse?
 - Piktogramme zeigen eine schnelle Übersicht.
 - Wir prüfen dabei auch die Angaben im Impressum.
- Datenschutzerklärung für Mitarbeitende:
 - Diese erklärt Ihren Mitarbeitenden, warum welche Daten benötigt werden.
 - Sie zeigt auf, wann diese Daten gelöscht werden müssen.



Beispiel Datenschutzerklärungen

■ Allgemeine Datenschutzerklärung

Datenschutzerklärung

Datenschutz und Datensicherheit sind wichtig für die aXenta ag («aXenta»; «wir»). Wir bearbeiten Ihre Personendaten verantwortungsbewusst, in Übereinstimmung mit anwendbaren gesetzlichen Bestimmungen und gemäss dieser Datenschutzerklärung.



Allgemeine
Personendaten



Überlassene Daten



Erhaltene Daten



Datenweitergabe

Inhalt dieser Datenschutzerklärung

In dieser Datenschutzerklärung informieren wir Sie darüber, wie wir Personendaten erheben und bearbeiten, wenn Sie unsere Website unter www.axenta.ch («Website») besuchen, uns kontaktieren oder unsere Leistungen in Anspruch nehmen.

Wir nutzen in der Datenschutzerklärung Privacy Icons. Weitere Informationen zu den Privacy Icons finden Sie unter privacy-icons.ch.

Verantwortlicher für die Datenbearbeitung

Für die in dieser Datenschutzerklärung beschriebenen Datenbearbeitungen ist aXenta verantwortlich.

Bei Fragen oder wenn Sie Ihre datenschutzrechtlichen Betroffenenrechte wahrnehmen möchten, kontaktieren Sie uns bitte über fabian.wipf@axenta.ch oder schreiben Sie an: Fabian Wipf, aXenta ag, Täferstrasse 5, 5405 Dättwil.

Bei der Kommunikation und Leistungserbringung bearbeitete Personendaten

Dazu gehören allgemeine Personendaten, z.B. Name und Kontaktdaten, sowie allenfalls Angaben zu Ihrer Position oder Rolle bei der Organisation, in deren Namen Sie uns kontaktieren.

Wir bearbeiten auch Personendaten, die wir von Dritten erhalten. Dazu gehören regelmässig Personendaten, die wir in der Korrespondenz oder in Besprechungen mit Kundinnen oder Geschäftspartnerinnen erhalten, z.B. Ihr Name und Angaben zu Ihrer Tätigkeit als Teammitglied der Kundin oder der Geschäftspartnerin.

Bereitstellung und Nutzung unserer Website

Nutzung zur Information

Sie können sich auf der Website über aXenta und unser Leistungsangebot informieren, ohne uns mitzuteilen, wer Sie sind. Wie bei jeder Verbindung mit einem Webserver, protokolliert und speichert der Server, auf dem wir die Website bereitstellen lassen, automatisch gewisse technische Daten und speichert sie für kurze Zeit. Dazu gehören die IP-Adresse und das Betriebssystem Ihres Geräts, das Datum und der Zeitpunkt der Nutzung sowie die Art des Browsers, über den Sie auf die Website zugreifen.

Zu welchen Zwecken wir Ihre Personendaten bearbeiten und auf welcher Basis

Ihre Personendaten bearbeiten wir primär, um über unser Leistungsangebot zu informieren und unsere Leistungen entsprechend unseren vertraglichen und gesetzlichen Pflichten zu erbringen, zu dokumentieren und abzurechnen.

Zudem bearbeiten wir Ihre Personendaten zu folgenden Zwecken:

- Beantwortung Ihrer Anfragen und Kommunikation mit Ihnen;
- Bereitstellung der Website;
- Erfüllung gesetzlicher Pflichten; und
- Durchsetzung von Rechtsansprüchen.

Wir haben ein den genannten Zwecken entsprechendes berechtigtes Interesse an der Bearbeitung Ihrer Personendaten. Einige Bearbeitungen sind zudem notwendig, damit wir unsere vertraglichen Pflichten Ihnen gegenüber oder unsere gesetzlichen Pflichten (z.B. Aufbewahrungspflichten) erfüllen können. Auf dieser Basis bearbeiten wir Ihre Personendaten, wenn und soweit das anwendbare Datenschutzrecht für die Rechtmässigkeit der Datenbearbeitung generell oder für bestimmte Bearbeitungstätigkeiten eine Rechtsgrundlage oder Rechtfertigung erfordert.

Wie wir Ihre Personendaten speichern und schützen

Wir speichern Ihre Personendaten nur in dem Umfang und so lange, wie dies für die Erfüllung der in dieser Datenschutzerklärung beschriebenen Zwecke oder zur Erfüllung gesetzlicher Pflichten notwendig ist.

Im Interesse der Integrität und der Vertraulichkeit der Personendaten treffen wir angemessene technische und organisatorische Massnahmen. Wir implementieren entsprechend unserer Risikobewertung insbesondere Zugangskontrollen, Zugriffskontrollen sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Massnahmen.

An wen wir Ihre Personendaten weitergeben

Zur Erreichung der in dieser Datenschutzerklärung beschriebenen Zwecke kann es notwendig sein, dass wir Ihre Personendaten an andere Unternehmen weitergeben. Es handelt sich um folgende Kategorien von Empfängerinnen:



Beispiel Datenschutzerklärungen

■ Datenschutzerklärung Mitarbeitende

aXenta Datenschutzerklärung für Mitarbeitende

Datenschutz und Datensicherheit sind wichtig für aXenta ag (nachfolgend: "aXenta"; "wir"). Wir bearbeiten Ihre Personendaten verantwortungsbewusst, in Übereinstimmung mit anwendbaren gesetzlichen Bestimmungen und gemäss unseren Datenschutzerklärungen.



Allgemeine Personendaten Finanzdaten Gesundheitsdaten



Überlassene Daten Erhaltene Daten Erhobene Daten Weltweit Datenweitergabe

- Inhalt dieser Datenschutzerklärung**

In dieser Datenschutzerklärung für Mitarbeitende informieren wir Sie darüber, wie wir Personendaten im Zusammenhang mit der Durchführung des Arbeitsverhältnisses über Sie erheben und bearbeiten.

Interne Richtlinien, Reglemente und Weisungen ergänzen diese Datenschutzerklärung.
- Verantwortlicher für die Datenbearbeitung**

Für die in dieser Datenschutzerklärung beschriebenen Datenbearbeitungen ist aXenta verantwortlich. Bei Fragen oder wenn Sie Ihre datenschutzrechtlichen Rechte als betroffene Person wahrnehmen möchten, wenden Sie sich bitte an die Datenschutzkontaktperson von aXenta:

Fabian Wipf
056-483 09 23
fabian.wipf@axenta.ch

3. Welche Personendaten wir zur Durchführung des Arbeitsverhältnisses erheben und bearbeiten

Damit wir unsere arbeitsvertraglichen und gesetzlichen Pflichten erfüllen können, müssen wir eine Reihe von Personendaten über Mitarbeitenden von aXenta bearbeiten. Dazu gehören:

- Namen, Adressen und Kontaktinformationen, inklusive E-Mail-Adresse und Telefonnummer;
- Geburtsdatum und Geschlecht;
- Anstellungsbedingungen und -verträge;
- Einzelheiten über die Qualifikation, Fähigkeiten und die Erfahrung unserer Mitarbeitenden sowie über den beruflichen Werdegang einschliesslich Start- und Enddaten bei ehemaligen Arbeitgeberinnen wie auch bei aXenta;
- Lohndaten, einschliesslich allfälliger Ansprüche auf Leistungen wie Renten oder aus Versicherungen;
- Bankverbindungen und Sozialversicherungsnummern;
- Daten über den Zivilstand, nächste Angehörige, Schutzbefohlene und Notfallkontakte;
- Daten über die Nationalität und gegebenenfalls die ausländerrechtliche Arbeitslaubnis;
- Einzelheiten über die vereinbarte Arbeitszeit (Arbeitstage und -stunden) sowie die effektiv geleistete Arbeit;
- Einzelheiten über Abwesenheiten, einschliesslich Urlaub, Krankheitstage, Mutter- oder Vaterschaftsurlaub und Sabbaticals sowie die Begründung für die Abwesenheit;
- Leistungsbeurteilungen einschliesslich der dazugehörigen Informationen, Informationen zu besuchten Weiterbildungen und Leistungszielen sowie die entsprechende Korrespondenz;
- Daten über medizinische und gesundheitliche Aspekte einschliesslich Informationen über allfällige Behinderungen, für die wir angemessene Arbeitsplatzanpassungen vornehmen müssen;
- Bild- und Tondaten; sowie
- Daten zur Nutzung von E-Mail, Internet und Dateisystemen von aXenta.

Die bearbeiteten Personendaten stammen aus verschiedenen Quellen, beispielsweise aus Bewerbungsformularen oder Lebensläufen; aus Reisepässen oder weiteren Identitätsdokumenten wie Fahrausweisen; aus Formularen, die Sie am Anfang oder während des Anstellungsverhältnisses ausgefüllt haben; aus Korrespondenz mit Ihnen oder aus Interviews, Besprechungen oder Beurteilungen.

In einigen Fällen bearbeiten wir Personendaten, die wir von Dritten erhalten, beispielsweise aus Referenzen vergangener Arbeitgeberinnen oder Informationen von "Background-Check"-Anbieterinnen, aus Bonitätsdatenbanken sowie aus rechtlich zulässigen Leumundsüberprüfungen.

Die bearbeiteten Personendaten speichern wir in verschiedenen Dateisystemen, insbesondere in Ihrem persönlichen Dossier sowie in Personal-Management- und weiteren



Richtlinien

- Interne Datenschutzrichtlinien:
 - Beschreibt die Datenschutzorganisation der Firma und hält Grundprinzipien fest.
- Technische und organisatorische Massnahmen:
 - Beschreibt Ihre technischen und organisatorischen Massnahmen, welche zum Schutz der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit von Personendaten getroffen werden.
- Richtlinien über die Datenaufbewahrung:
 - Beschreibt, wer für die Daten verantwortlich ist.
 - Definiert, wie lange welche Daten aufbewahrt werden.



Beispiel Richtlinien

■ Interne Datenschutzrichtlinie

aXenta ag Interne Datenschutzrichtlinie

1. Gegenstand und Zweck

Datenschutz und Datensicherheit sind wichtig für die aXenta ag (nachfolgend: «**aXenta**»). Diese interne Datenschutzrichtlinie («**Richtlinie**») beschreibt die Datenschutzorganisation der aXenta und hält die Grundprinzipien fest, nach denen aXenta Personendaten bearbeitet.

Die festgelegten Grundsätze und Verhaltensanweisungen unterstützen aXenta bei der Einhaltung der Anforderungen des anwendbaren Datenschutzrechts.

2. Geltungsbereich

Diese Richtlinie gilt für alle internen und externen Mitarbeitenden der aXenta.

3. Definitionen

Diese Richtlinie verwendet datenschutzrechtliche Begriffe, die sich an den gesetzlichen Definitionen orientieren. Sie bedeuten das Folgende:

- **Personendaten** sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen; als bestimmbar wird eine natürliche Person angesehen, wenn aXenta oder Empfängerinnen der Daten die natürliche Person aufgrund der Angaben direkt oder indirekt identifizieren können. Dazu gehören in der Regel allgemeine Personendaten wie Name, Vorname und Kontaktdaten sowie Kundennummern und andere Kennungen (z.B. die aXenta-Kundennummer), die aXenta über die betroffene Person (z.B. eine Mitarbeiterin oder Kundin der aXenta) erhebt und bearbeitet. Ausserdem gehören dazu Finanzdaten und Gesundheitsdaten, die sich auf eine betroffene Person beziehen.
- **Besonders schützenswerte Personendaten** sind die folgenden Kategorien von besonders sensiblen Personendaten: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie; genetische Daten; biometrische Daten, die eine natürliche Person eindeutig identifizieren; Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe.
- **Betroffene Person** ist die natürliche Person, über die Personendaten bearbeitet werden.
- **Bearbeiten** bedeutet jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Personendaten.

Beispiel Richtlinien

- Technische und organisatorische Massnahmen

aXenta ag Technische und organisatorische Massnahmen

(A) Allgemeine Bestimmungen

Dieses Dokument beschreibt die technischen und organisatorischen Massnahmen, welche aXenta ag zum Schutz der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit von Personendaten trifft.

(B) Technische und organisatorische Sicherheitsmassnahmen

1. Vertraulichkeit

1.1. Zugangskontrolle

"Unbefugten ist der (räumliche) Zutritt zu Datenverarbeitungsanlagen, in denen Kundendaten (einschliesslich Personendaten) verarbeitet werden oder genutzt werden, zu verwehren."

Umgesetzte Massnahmen:
Massnahmen Zutrittskontrolle

1.2. Benutzerkontrolle

"Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können."

Umgesetzte Massnahmen:
Massnahmen Zugangskontrolle

1.3. Zugriffskontrolle und Speicherkontrolle

"Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die zur Erfüllung ihrer Aufgaben notwendigen (Need-to-Know) und ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Kundendaten (einschliesslich Personendaten) bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können."

Umgesetzte Massnahmen:
Massnahmen Zugriffskontrolle

2. Integrität

2.1. Weitergabekontrolle (Transportkontrolle, Datenträgerkontrolle und Bekanntgabekontrolle)

"Es ist zu gewährleisten, dass Personendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen,

Beispiel Richtlinien

■ Richtlinien über die Datenaufbewahrung

aXenta ag Richtlinie zur Datenaufbewahrung

1. Geltungsbereich

Alle Aufzeichnungen der aXenta ag ("aXenta"), ob analog oder digital, unterliegen den Aufbewahrungsanforderungen dieser Richtlinie.

2. Zuständigkeit und Verantwortlichkeiten

Ariane Senn ist für die Aufbewahrung finanzieller und damit zusammenhängender Unterlagen (wie Buchhaltung, Steuern) verantwortlich. In diesem Zusammenhang bedeutet Aufbewahrung, sicherzustellen, dass aXenta die Dokumente, die aXenta gemäss gesetzlichen Pflichten aufbewahren muss, aufbewahrt und zur Archivierung übergibt.

Ariane Senn ist für die Aufbewahrung aller Personalunterlagen, einschliesslich der Gesundheits- und Sicherheitsaufzeichnungen, verantwortlich.

Ariane Senn ist für die Aufbewahrung aller anderen übrigen Unterlagen verantwortlich, für die eine gesetzliche Aufbewahrungspflicht besteht oder an deren Aufbewahrung aXenta ein berechtigtes Geschäftsinteresse (z.B. Geschäftskontinuität) hat.

Marc Stäger ist verantwortlich für die Speicherung aller Daten gemäss dieser Richtlinie und dafür, dass die aufbewahrten Aufzeichnungen in die Pläne für Geschäftskontinuität und Notfallwiederherstellung (Business Continuity und Disaster Recovery) aufgenommen werden.

3. Aufbewahrungsfristen

Das anwendbare Recht legt Mindestaufbewahrungsfristen für verschiedene Arten von Dokumentationen fest. aXenta muss alle diese Unterlagen identifizieren (manchmal mithilfe einer Behörde - z.B. kann die Aufbewahrung von Steuerunterlagen für einen anderen Zeitraum erforderlich sein als andere Buchhaltungsunterlagen) und für diese Mindestaufbewahrungsfristen festlegen. Es kann Umstände geben, unter denen eine interne Risikobewertung ergibt, dass längere Aufbewahrungsfristen erforderlich sind.

Die erforderlichen Aufbewahrungsfristen nach Datensatz-Typ sind derzeit wie folgt:

Prozessbeschreibungen

- Prozessbeschreibung im Umgang mit Betroffenenrechten:
 - Dieses Dokument definiert diese Abläufe und Verantwortlichkeiten im Zusammenhang mit der Bearbeitung von Anfragen zur Ausübung von Betroffenenrechten.
- Prozessbeschreibung Datensicherheits-Verletzung:
 - Dieses Dokument stellt sicher, dass Sie bei einer Datensicherheits-Verletzung angemessen und effektiv reagieren.
- Prozessbeschreibung Datenschutz-Risikoanalyse:
 - Dieses Dokument stellt sicher, dass Sie mögliche Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten identifizieren und geeignete Massnahmen ergreifen, um diese Risiken zu minimieren.



Beispiel Prozessbeschreibungen

■ Prozessbeschreibung im Umgang mit Betroffenenrechten

Prozessbeschreibung betreffend Umgang mit Betroffenenbegehren

1. Einleitung

Betroffene Personen – z.B. Mitarbeitende oder Kundinnen der aXenta ag («aXenta») – haben unter den anwendbaren Datenschutzgesetzen eine Reihe von Rechten. Dazu gehören das Auskunftsrecht, das Recht auf Datenherausgabe oder -übertragung sowie das Recht auf Berichtigung oder Löschung («Betroffenenrechte»).

2. Zweck dieser Prozessbeschreibung

Diese Prozessbeschreibung dient der Datenschutzkontaktperson der aXenta als Leitlinie zur Prüfung von Anfragen betroffener Personen betreffend Ausübung von Betroffenenrechten («Betroffenenbegehren»).

3. Prozess im Allgemeinen

3.1. Entgegennahme

Mitarbeitende der aXenta leiten Betroffenenbegehren gemäss interner Datenschutzrichtlinie an die Datenschutzkontaktperson weiter. Die Datenschutzkontaktperson nimmt die Begehren entgegen und sorgt für ihre Bearbeitung.

3.2. Verzeichnis der Betroffenenbegehren

Die Datenschutzkontaktperson führt ein Verzeichnis der Betroffenenbegehren. Darin notiert sie Name und Vorname der betroffenen Person sowie das Datum des Eingangs und der Beantwortung jedes Betroffenenbegehrens.

3.3. Schriftlichkeit

Bei mündlichen Betroffenenbegehren verlangt die Datenschutzkontaktperson von der betroffenen Person, dass diese das Begehren schriftlich stellt.

3.4. Identitätsnachweis

Eine betroffene Person kann Betroffenenbegehren nur in Bezug auf sie betreffende Personendaten stellen. Sie kann das Betroffenenbegehren selbst stellen oder in ihrem Namen stellen lassen.

Die Datenschutzkontaktperson stellt sicher, dass die betroffene Person, einen ausreichenden Identitätsnachweis erbracht hat. Stellt ein Dritter (z.B. Rechtsanwalt oder Bezugsperson) das Begehren im Namen einer betroffenen Person, so muss der Dritte den Nachweis erbringen, dazu ermächtigt zu sein (Vollmacht).



Beispiel Prozessbeschreibungen

■ Prozessbeschreibung Datensicherheits-Verletzung

Prozessbeschreibung betreffend Umgang mit Datensicherheits-Verletzungen ("Data Breaches") aXenta ag

1. Einleitung

aXenta («aXenta ag») ist je nach Art und Schwere von Verletzungen der Datensicherheit verpflichtet, die zuständige Datenschutzaufsichtsbehörde («Behörde») und (gegebenenfalls) die betroffenen Personen über eine Verletzung der Datensicherheit zu informieren.

«Verletzung der Datensicherheit» bedeutet eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

aXenta ag bearbeitet auch Personendaten im Auftrag, nach Weisungen und für Zwecke anderer Gesellschaften («Auftragsdaten»). Wenn die Verletzung der Datensicherheit (auch) Auftragsdaten betrifft, ist aXenta ag zur Meldung an die verantwortlichen Gesellschaften verpflichtet.

2. Zweck dieser Prozessbeschreibung

Diese Prozessbeschreibung betreffend Umgang mit Verletzungen der Datensicherheit («Prozessbeschreibung») dient der Datenschutzkontaktperson dazu, festgestellte Verletzungen der Datensicherheit zu untersuchen, eine Risikoanalyse durchzuführen und Verletzungen der Datensicherheit gegebenenfalls der Behörde sowie betroffenen Personen zu melden.

3. Entgegennahme interner Meldungen und Untersuchung

Die Datenschutzkontaktperson erhält Meldungen festgestellter Verletzungen der Datensicherheit per Telefon 056-483 09 23, ergänzt durch E-Mail an fabian.wipf@axenta.ch. Nach Eingang einer Meldung informiert der Datenschutzkontaktperson die Leitung ICT («Leitung ICT»).

Die Leitung ICT unterstützt die Datenschutzkontaktperson bei der Untersuchung der Verletzung der Datensicherheit. Stellt die Leitung ICT selber eine Verletzung der Datensicherheit fest, informiert er umgehend die Datenschutzkontaktperson.

4. Risikoanalyse

Die Datenschutzkontaktperson und die Leitung ICT prüfen gemeinsam, ob eine festgestellte Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte betroffener Personen führt. Sie beraten die Geschäftsleitung hinsichtlich des Entscheids, die Verletzung der Datensicherheit an die Behörde und/oder die betroffenen Personen zu melden.



Beispiel Prozessbeschreibungen

■ Prozessbeschreibung Datenschutz-Risikoanalyse

Prozessbeschreibung betreffend Datenschutz-Risikoanalyse

1. Geltungsbereich und Zweck

aXenta ag (aXenta) wendet diese Prozessbeschreibung betreffend Datenschutz-Risikoanalyse («**Prozessbeschreibung**») zur Beurteilung der Datenschutzrisiken eines neuen Projekts bzw. der Einführung einer neuen oder geänderten Bearbeitungstätigkeit an.

Die Checkliste bietet eine Anleitung insbesondere im Hinblick auf die Feststellung, ob eine Datenschutz-Folgenabschätzung («**DSFA**») – und allenfalls eine Vorabkonsultation der zuständigen Datenschutzaufsichtsbehörden – erforderlich ist.

2. Entgegennahme von Projektmeldungen

2.1. Projektverantwortliche melden neue Projekte bzw. neue Bearbeitungstätigkeiten vor ihrer Einführung an die Leitung ICT («**Leitung ICT**») wie auch an die Datenschutzkontaktperson der aXenta.

2.2. Die Datenschutzkontaktperson sorgt dafür, dass Projektverantwortliche den folgenden Fragebogen ausfüllen, wertet die Anfragen in Abstimmung mit der Leitung ICT aus und unterstützt die Geschäftsleitung oder den jeweiligen Steuerungsausschuss beim Entscheid, eine DSFA durchzuführen.

3. Fragebogen

Die folgenden Fragen sollen bei der Entscheidung helfen, ob eine DSFA erforderlich ist. Wenn neben der ersten Frage eine weitere mit «Ja» beantwortet wird, ist dies ein Hinweis darauf, dass die Durchführung einer DSFA angezeigt ist.

Projekt Name

Projekt Beschreibung

4. Projekt

4.1. Wird das Projekt die Sammlung neuer Informationen über betroffene Personen beinhalten?

Informationen Betroffene Personen

5. Administrative Informationen

Datum: Datum

Ausgefüllt von:

Signatur

Funktion



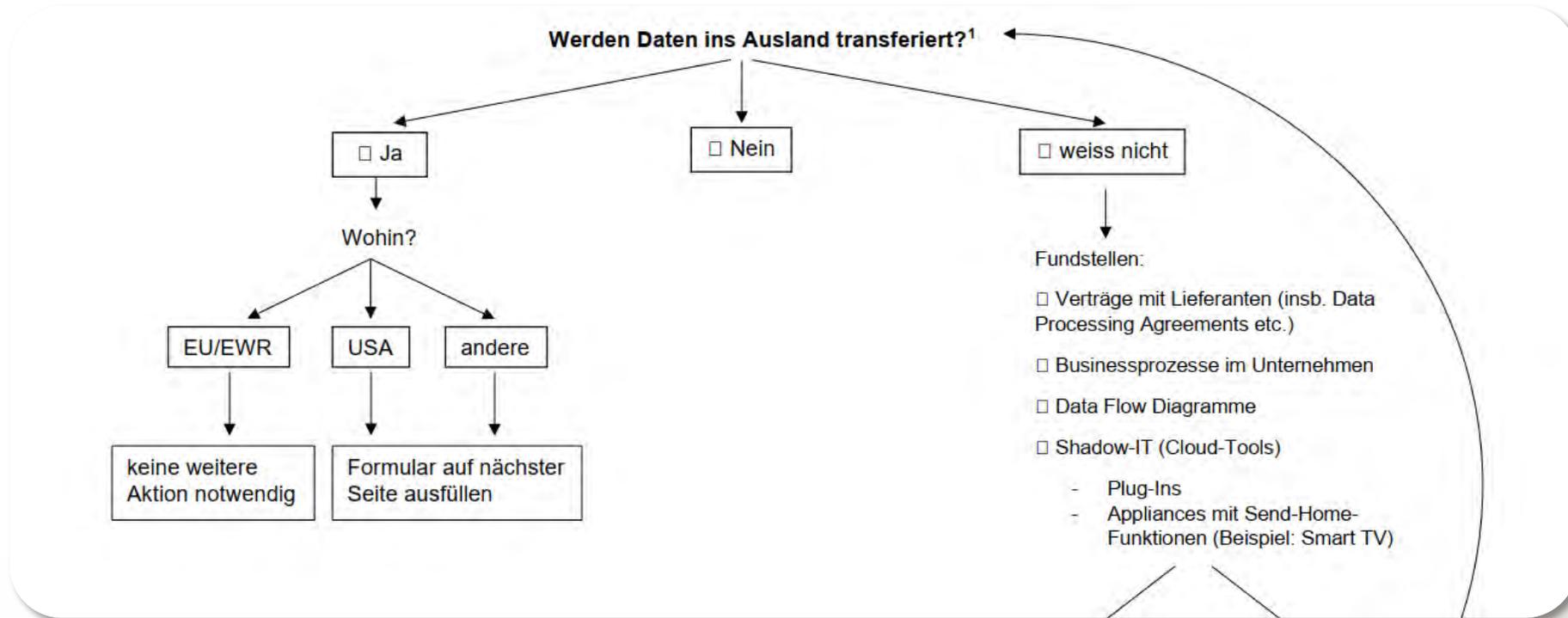
Checkliste & Musterschreiben

- Checkliste grenzüberschreitende Datenbekanntgabe:
 - Die Checkliste identifiziert, wo Daten ins Ausland transferiert werden, damit die besonderen Anforderungen an den Datenschutz eingehalten werden.
- Checkliste Auftragsbearbeitung:
 - Diese Checkliste identifiziert, mit wem Sie einen Auftragsbearbeitungsvertrag abschliessen müssen und wie vorzugehen ist.
- Musterschreiben Antwort Betroffenenrechte:
 - Sie erhalten mehrere Briefe für die Antworten an Ihre Versicherten.
- Checkliste Umsetzung Datenschutzgesetz:
 - Eine Checkliste zur Umsetzung darf auch nicht fehlen.



Beispiel Checkliste & Musterschreiben

- Checkliste grenzüberschreitende Datenbekanntgabe



Beispiel Checkliste & Musterschreiben

■ Checkliste Auftragsbearbeitung

2. Szenario: SIE möchten, dass ein Dienst-Anbieter (Dienstleister) eine ADV mit Ihnen abschliesst

Hinweis: Dieses Szenario gilt vor allem in Situationen, in denen Sie für die Bearbeitung Ihrer Personendaten einen Dienstleister (z.B. ein Anbieter von Cloud-Diensten oder ein Web-Hoster) beiziehen möchten.

Gehen Sie diese Checkliste durch, um festzustellen, ob eine ADV erforderlich ist:

(1) Personendaten

Geben Sie Personendaten an den Dienstleister weiter?

- wenn NEIN: Keine Notwendigkeit einer ADV.
- wenn JA: Fahren Sie mit der nächsten Frage fort. Notwendigkeit einer ADV prüfen.

Sind weitere Personendaten als nur Kontaktdaten Ihrer eigenen Mitarbeitenden betroffen? (Beispiel: Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Adresse der Mitarbeitenden Ihrer Kunden oder anderen Geschäftspartner)

- wenn NEIN: Keine Notwendigkeit einer ADV.

Erläuterung: Der Dienstleister wird diese Kontaktdaten (z.B. Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Adresse des Dienstleisters) in sein Customer Relationship Management System (CRM) eingeben und zum Zwecke der Fortführung der Geschäftsbeziehung bearbeiten. Dies ist ein echtes Interesse des Dienstleisters. Mit anderen Worten: Der Dienstleister tut dies nicht zu Ihren Gunsten (nicht "in Ihrem Auftrag"). Daher ist der Dienstleister der Verantwortliche (und in dieser Hinsicht kein Auftragsbearbeiter). Es ist jedoch wichtig, dass Sie die Kontaktdaten (Personendaten) Ihrer Mitarbeitenden nur dann an dem Dienstleister weitergeben, wenn dies aus geschäftlichen Gründen erforderlich ist. Sie bleiben natürlich Ihrerseits (in Ihrem Einfluss- und Verantwortungsbereich) Verantwortlicher unter dem Datenschutzgesetz in Bezug auf die Bearbeitung der Personendaten über Ihre Mitarbeitenden.

- wenn JA: Fahren Sie mit der nächsten Frage fort. Notwendigkeit einer ADV prüfen.

(2) Bearbeitung durch einen Dienstleister in Ihrem Auftrag

Ist die Bearbeitung der Personendaten Teil einer Dienstleistung, die Sie vom Dienstleister erhalten (z.B. damit Sie von einer Aufgabe entlastet werden, die Sie sonst selbst ausgeführt hätten)?

- wenn NEIN: Keine Notwendigkeit einer ADV.

Beispiel: Wenn Sie Personendaten z. B. an Banken (zur Durchführung von Zahlungen usw.) oder an Steuerbehörden (z. B. im Zusammenhang mit der Meldung der Mehrwertsteuer usw.) weitergeben, gelten diese Empfänger von Personendaten aus Ihrer Sicht nicht als Auftragsbearbeiter. Diese Personendaten werden an diese Stellen in ihrer Eigenschaft als Verantwortliche übermittelt (Übermitt-

Beispiel Checkliste & Musterschreiben

- Musterschreiben Antwort
Betroffenenrechte

Musterschreiben für die Beantwortung von Betroffenenbegehren

Einleitung

Das Schweizer Datenschutzgesetz (DSG) gewährt betroffenen Personen – z.B. Mitarbeitenden, Kundinnen oder Kunden – eine Reihe von Rechten. Dazu gehören das Auskunftsrecht, das Recht auf Datenherausgabe oder -übertragung sowie das Recht auf Berichtigung oder Löschung («**Betroffenenrechte**»).

Der Beantwortungsprozess ist in der «Prozessbeschreibung betreffend Umgang mit Betroffenenbegehren» («**Prozessbeschreibung**») genauer beschrieben. Die nachfolgenden Musterschreiben und Textbausteine dienen der Beantwortung solcher Begehren.

Beantwortung eines einfachen Auskunftsbegehrens

Sehr geehrter Herr Peter Muster

Ihr Begehren auf Auskunft haben wir am 22. Februar 2023 erhalten.

Innerhalb der anwendbaren Frist von 30 Tagen erteilen wir Ihnen nachfolgend die gewünschte Auskunft zu den Sie betreffenden Personendaten.

Diese Personendaten bearbeiten wir zu folgenden Zwecken:

Bearbeitungszwecke.

Wir speichern diese Personendaten Speicherdauer oder Kriterien.

Wir haben Ihre Personendaten aus folgenden Quellen erhalten:

Beispiel Checkliste & Musterschreiben

- Checkliste Umsetzung Datenschutzgesetz

Neues DSG – die 7 To-dos

- (1) Erstellen Sie ein Bearbeitungsverzeichnis – es wird Ihnen helfen
- (2) Transparenz! Erstellen Sie eine Datenschutzerklärung für Kundinnen und andere Kontakte
- (3) Transparenz! Erstellen Sie eine Datenschutzerklärung für Mitarbeitende
- (4) Organisieren Sie sich, um rasch auf Fragen antworten zu können

Vendor Management

- Datenschutz-Fragebogen für Drittdienstleister:
 - Ihr Instrument zum Sicherzustellen, dass Drittdienstleister Ihre Datenschutzstandards und Anforderungen einhalten.
- Vereinbarung zur Auftragsbearbeitung ADV:
 - Die Vereinbarung konkretisiert die Rechte und Pflichten der Parteien im Bezug auf die Auftragsbearbeitung.
- EU-Standard-Vertragsklauseln zur Auftragsverarbeitung
- EU-Standard-Vertragsklauseln zur grenzüberschreitenden Datenbekanntgabe:
 - Standardverträge die von der Europäischen Kommission erstellt wurden.



Beispiel Vendor Management

- Datenschutz-Fragebogen für Drittdienstleister

Datenschutz-Fragebogen für Lieferantinnen

Unternehmen Firma will ihrer Lieferantinnen sorgfältig auswählen und instruieren, um die Regeln des auf unsere Bearbeitungstätigkeiten anwendbaren Datenschutzrechts einzuhalten. Aus diesem Grund bitten wir Sie, diesen Fragebogen wahrheitsgemäss und so detailliert wie möglich auszufüllen.

- 1. Informationen zu Ihrem Unternehmen**
Firma Lieferantin
Adresse Lieferantin
- 2. Kontaktdaten**
- 3. Dienstleistung**
Beratung und Cloud Dienstleistung rund um infonIQ
- 4. Bearbeitung Personendaten**
Wir bearbeiten im Rahmen unserer Dienstleistung keine Personendaten für Unternehmen Firma.
- 5. Datenschutzerklärung**
Link zu Datenschutzerklärung
- 6. Subunternehmen**
Wir verwenden keine Subunternehmen.
- 7. Technische und organisatorische Massnahmen**
TO Massnahmen
- 8. Pseudonymisierung & Verschlüsselung**
Pseudonymisierung und Verschlüsselung
- 9. Speicherung und Aufbewahrung von Personendaten**
Speicherung und Aufbewahrung Daten
- 10. Rolle Drittdienstleister**
Auftragsbearbeiter
- 11. Verantwortliche Person bei Unternehmen Firma**
Kontakt

Beispiel Vendor Management

- Vereinbarung zur Auftragsbearbeitung ADV

Vereinbarung zur Auftragsbearbeitung

zwischen
Crystal Vorsorge
Demostrasse 12
8200 Schaffhausen

Kundin

und

Name Anbieterin
Adresse Anbieterin

Anbieterin

(Kundin und Anbieterin je einzeln eine "Partei" und zusammen die "Parteien")

A. Allgemeine Bestimmungen

1 Gegenstand und Anwendungsbereich dieser Vereinbarung

1.1 Diese Vereinbarung über die Auftragsbearbeitung ("**Vereinbarung**") konkretisiert die Rechte und Pflichten der Parteien in Bezug auf die Auftragsbearbeitung, die sich für sie aus dem anwendbaren Datenschutzrecht ergeben. Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen zwischen den Parteien. Dabei kann es sich um einen einzelnen oder mehrere Verträge zwischen den Parteien über die Leistungserbringung für die Kundin handeln ("**Vertrag**").

1.2 Die Vereinbarung gilt nur in Bezug auf Dienstleistungen, bei denen die Anbieterin Personendaten im Auftrag und für Zwecke der Kundin bearbeitet ("**Auftragsbearbeitung**"), wobei die Kundin entweder Verantwortliche oder Auftragsbearbeiterin und die Anbieterin entweder Auftragsbearbeiterin oder Unter-Auftragsbearbeiterin ist.

1.3 Diese Vereinbarung ist ein integraler Bestandteil des Vertrags. Die Bestimmungen dieser Vereinbarung schränken die Rechte und Pflichten der Parteien in Bezug auf die Erbringung von Dienstleistungen unter dem Vertrag nicht ein. Ihren Regelungsgegenstand betreffend gehen die Bestimmungen dieser Vereinbarung indes den Bestimmungen des Vertrags vor.

Beispiel Vendor Management

- EU-Standard-Vertragsklauseln zur Auftragsverarbeitung

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

((a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

((b) The controller and processor listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

((c) These Clauses apply to the processing of personal data as specified in Annex II.

((d) Annexes I to IV are an integral part of the Clauses.

((e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

((f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

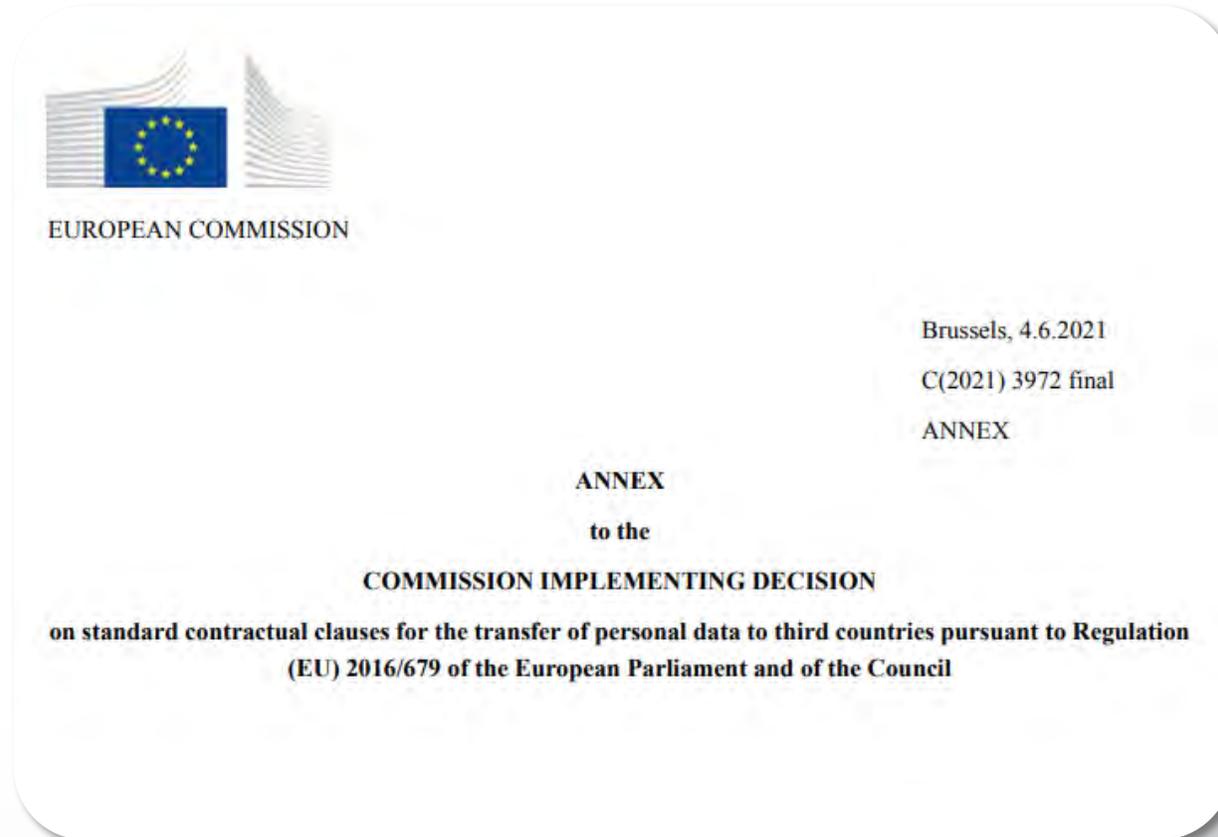
Invariability of the Clauses

((a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

((b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Beispiel Vendor Management

- EU-Standard-Vertragsklauseln zur grenzüberschreitenden Datenbekanntgabe



Kontaktieren Sie uns



Michael Flückiger

Geschäftsleiter (CEO)

E-Mail: michael.flueckiger@axenta.ch

Telefon: +41 56 483 09 00



Fabian Wipf

Information Security Officer

E-Mail: fabian.wipf@axenta.ch

Telefon: +41 56 483 09 23



Vielen Dank für Ihre Aufmerksamkeit!

Thank
You