Auftragsbearbeitungsvertrag ADV

Letzte Aktualisierung: 22.9.2023

Sprache: DE

Kontera GmbH

Struktur

Dieser ADV ist wie folgt aufgebaut:

Begriff	
Abschnitt A – Details der Datenverarbeitung	Die wichtigsten Definitionen und Details der Datenbearbeitung im Rahmen dieser ADV sind in Abschnitt A festgelegt.
Abschnitt B – Geltungsbereich	Enthält die für die Vereinbarung geltenden allgemeinen rechtlichen Bestimmungen.
Abschnitt C – TOMs	Die anwendbaren technischen und organisatorischen Massnahmen.

Abschnitt A – Details der Datenverarbeitung

Begriff	Definition
Verantwortlicher	
Auftragsbearbeiter	Kontera GmbH Bleicheweg 3 4802 Strengelbach Kontakt: dpa@kontera.ch (gemeinsam mit dem Verantwortlichen die „Parteien“)
Processing purpose	Verarbeitung im Zusammenhang mit: https://kontera.ch/legal/docs/tos datiert 1. März 2023 (der “Basisvertrag”)
Dauer der Bearbeitung	So lange wie für den Basisvertrag erforderlich
Kategorien von betroffenen Personen	Kunden
Kategorien von Personendaten	Kontoangaben und finanzielle Daten
Ort der Speicherung und Bearbeitung	An der Geschäftsadresse des Auftragsbearbeiters und seiner genehmigten Unterauftragsbearbeiter wie in diesem ADV erwähnt.
Vor-Ort-Prüfungen	Nein
Unterauftragsbearbeiter	Unterauftragsbearbeiter sind hier aufgeführt: https://kontera.ch/legal/docs/subprocessors
Übermittlungen ausserhalb der EU/EWR/Schweiz	Übermittlung ausserhalb von EU/EWR/Schweiz sind nur für Länder zulässig, in denen der Auftragsbearbeiter oder ein zugelassener Unterauftragsbearbeiter registriert ist

Die in Abschnitt A definierten Variablen dienen als Definitionen in Abschnitt B.

Abschnitt B – Geltungsbereich

1. Zweck und Anwendungsbereich

a) Zweck dieses Auftragsbearbeitungsvertrags (ADV) ist es, die Einhaltung von Artikel 28 Absätze 3 und 4 der EU-Datenschutz-Grundverordnung (DSGVO) und Artikel 9 des Schweizerischen Bundesgesetzes über den Datenschutz (DSG) zu gewährleisten, und zwar in Bezug auf jedes Gesetz nur dann und in dem Umfang, der auf die jeweilige Bearbeitungstätigkeit anwendbar ist.

b) Dieser ADV gilt für die Verarbeitung personenbezogener Daten gemäss Abschnitt A.

2. Auslegung

a) Wo in diesem ADV Begriffe verwendet werden, die in der Datenschutz-Grundverordnung oder im DSG definiert sind, haben diese Begriffe dieselbe Bedeutung wie in diesen Gesetzen.

b) Dieser ADV ist im Lichte der Bestimmungen der DSGVO und des DSG zu lesen und auszulegen, soweit diese anwendbar sind.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die im Widerspruch zu den Rechten und Pflichten steht, die in der DSGVO bzw. im DSG vorgesehen sind, oder die Grundrechte oder -freiheiten der betroffenen Personen beeinträchtigt.

3. Hierachie

Im Falle eines Widerspruchs zwischen diesem ADV und den Bestimmungen einer anderen Vereinbarung zwischen den Parteien, die zum Zeitpunkt der Vereinbarung dieses ADV besteht oder danach abgeschlossen wird, hat dieser ADV Vorrang, es sei denn, es wurde ausdrücklich etwas anderes in Textform vereinbart.

4. Beschreibung der Bearbeitung(en)

Die Einzelheiten der Bearbeitungen, insbesondere die Kategorien personenbezogener Daten und die Zwecke der Verarbeitung, für die die Personendaten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet werden, sind in Abschnitt A aufgeführt.

5. Verpflichtungen der Vertragsparteien

5.1 Allgemein

a) Der Auftragsbearbeiter verarbeitet Personendaten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen, es sei denn, er ist aufgrund von Rechtsvorschriften der EU, der Mitgliedstaaten oder der Schweiz, denen der Auftragsbearbeiter unterliegt, hierzu verpflichtet. Solche Weisungen sind in Abschnitt A aufgeführt. In diesem Fall unterrichtet der Auftragsbearbeiter den für die Verarbeitung Verantwortlichen vor der Verarbeitung über diese rechtliche Verpflichtung, es sei denn, das Gesetz verbietet dies aus wichtigen Gründen des öffentlichen Interesses. Der für die Verarbeitung Verantwortliche kann während der gesamten Dauer der Verarbeitung von Personendaten auch nachträgliche Weisungen erteilen. Solche Weisungen sind stets zu dokumentieren.

b) Der Auftragsbearbeiter unterrichtet den für die Verarbeitung Verantwortlichen unverzüglich, wenn die Anweisungen des für die Verarbeitung Verantwortlichen nach Ansicht des Auftragsbearbeiter gegen geltende Datenschutzvorschriften der EU, der Mitgliedstaaten oder der Schweiz verstossen.

5.2 Zweckbindung

Der Auftragsbearbeiter verarbeitet die Personendaten nur für den/die in Abschnitt A genannten Zweck(e) der Verarbeitung.

5.3 Löschung oder Rückgabe von Daten

a) Die Verarbeitung durch den Auftragsbearbeiter darf nur für die in Abschnitt A angegebene Dauer erfolgen.

b) Bei Beendigung der Erbringung von Dienstleistungen zur Verarbeitung von Personendaten oder bei Beendigung gemäss Klausel 8 hat der Auftragsbearbeiter alle im Auftrag des für die Verarbeitung Verantwortlichen verarbeiteten Personendaten zu löschen und dem für die Verarbeitung Verantwortlichen zu bescheinigen, dass er dies getan hat und vorhandene Kopien löschen, es sei denn, das EU-Recht, das Recht der Mitgliedstaaten oder das schweizerische Recht schreibt die Aufbewahrung der Personendaten vor.

5.4 Sicherheit der Verarbeitung

a) Der Auftragsbearbeiter ergreift die in Abschnitt C genannten technischen und organisatorischen Massnahmen, um die Sicherheit der Personendaten zu gewährleisten, einschliesslich des Schutzes vor zufälliger oder unrechtmässiger Zerstörung, Verlust, Veränderung, unbefugter Weitergabe oder unbefugtem Zugriff auf diese Daten (Verletzung des Schutzes von Personendaten) gemäss Art. 5, Art. 28, Abs. 3. lit c, und Art. 32 GDPR und Art. 8 DSG. Bei der Beurteilung des angemessenen Sicherheitsniveaus berücksichtigen sie insbesondere die mit der Verarbeitung verbundenen Risiken, die Art der Personendaten sowie Art, Umfang, Kontext und Zwecke der Verarbeitung.

b) Im Falle einer Verletzung des Schutzes von Personendaten in Bezug auf Daten, die vom Auftragsbearbeiter verarbeitet werden, benachrichtigt dieser den für die Verarbeitung Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem er von der Verletzung Kenntnis erhalten hat. Diese Benachrichtigung enthält die Angaben zu einer Kontaktstelle, bei der weitere Informationen über die Verletzung des Schutzes von Personendaten eingeholt werden können, eine Beschreibung der Art der Verletzung (einschliesslich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze), ihrer wahrscheinlichen Folgen und der Massnahmen, die zur Minderung ihrer möglichen nachteiligen Auswirkungen ergriffen wurden oder ergriffen werden sollen. Ist es nicht möglich, alle Informationen gleichzeitig zur Verfügung zu stellen, so enthält die erste Benachrichtigung die zu diesem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden ohne unangemessene Verzögerung bereitgestellt, sobald sie verfügbar sind.

c) Der Auftragsbearbeiter arbeitet nach Treu und Glauben mit dem für die Verarbeitung Verantwortlichen zusammen und unterstützt ihn in jeder erforderlichen Weise, damit der für die Verarbeitung Verantwortliche gegebenenfalls die zuständige Datenschutzbehörde und die betroffenen Personen benachrichtigen kann, wobei die Art der Verarbeitung und die dem Auftragsbearbeiter zur Verfügung stehenden Informationen berücksichtigt werden.

d) Der Auftragsbearbeiter gewährt seinen Mitarbeitern nur insoweit Zugang zu den Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsbearbeiter stellt sicher, dass die Personen, die zur Verarbeitung der erhaltenen

Personendaten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

e) Betrifft die Bearbeitung Personendaten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über Gesundheit oder das Sexualleben oder die sexuelle Ausrichtung einer Person, Daten über Massnahmen der sozialen Hilfe oder Daten über strafrechtliche Verurteilungen und Straftaten (besondere Datenkategorien), so wendet der Auftragsbearbeiter besondere Beschränkungen und/oder zusätzliche Garantien an, die der für die Verarbeitung Verantwortliche angemessenerweise verlangt.

5.5 Dokumentation und Einhaltung der Vorschriften

a) Die Parteien müssen in der Lage sein, die Einhaltung dieses ADV nachzuweisen.

b) Der Auftragsbearbeiter ist verpflichtet, alle angemessenen Anfragen des für die Datenverarbeitung Verantwortlichen, die sich auf die Verarbeitung im Rahmen dieser DSGVO beziehen, unverzüglich und ordnungsgemäss zu beantworten.

c) Der Auftragsbearbeiter stellt dem für die Verarbeitung Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesem ADV festgelegten und sich unmittelbar aus der DSGVO oder dem DSG ergebenden Verpflichtungen nachzuweisen, und ermöglicht auf Verlangen des für die Verarbeitung Verantwortlichen die Überprüfung von Dateien und Unterlagen oder von Audits der unter diese Klauseln fallenden Bearbeitungstätigkeiten und trägt dazu bei, insbesondere wenn es Anzeichen für eine Nichteinhaltung gibt.

d) Der für die Verarbeitung Verantwortliche hat die Wahl, das Audit selbst durchzuführen, auf eigene Kosten einen unabhängigen Prüfer zu beauftragen oder sich auf ein vom Auftragsbearbeiter beauftragtes unabhängiges Audit zu verlassen. Beauftragt der Auftragsbearbeiter ein Audit, so hat er die Kosten für den unabhängigen Prüfer zu tragen. Die Audit-, Zugangs- und Inspektionsrechte des für die Verarbeitung Verantwortlichen gemäss dieser Klausel beschränken sich ausschliesslich auf die Aufzeichnungen des Auftragsbearbeiter (einschliesslich u. a. der Verzeichnisse der

Tätigkeiten zur Verarbeitung personenbezogener Daten und der Verzeichnisse der Empfänger personenbezogener Daten) und gelten nicht für die physischen Räumlichkeiten des Auftragsbearbeiter. Jede Prüfung und jedes Auskunftsersuchen ist auf die Informationen zu beschränken, die für die Zwecke dieses ADV erforderlich sind, und hat den Vertraulichkeitsverpflichtungen des Auftragsbearbeiter und seinem berechtigten Interesse am Schutz von Geschäftsgeheimnissen gebührend Rechnung zu tragen.

e) Der Auftragsbearbeiter und der für die Verarbeitung Verantwortliche stellen die in dieser Klausel genannten Informationen, einschliesslich der Ergebnisse etwaiger Audits, der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung, wenn und soweit dies nach der DSGVO oder dem DSG erforderlich ist.

5.6 Einsatz von Unterauftragsbearbeitern

a) Der Auftragsbearbeiter verfügt über die allgemeine Ermächtigung des für die Verarbeitung Verantwortlichen für die Beauftragung von Unterauftragsbearbeitern. Die Liste der Unterauftragsbearbeiter des Auftragsbearbeiter ist in Abschnitt A zu finden. Der Auftragsbearbeiter unterrichtet den für die Verarbeitung Verantwortlichen in Textform mindestens 30 Tage im Voraus über beabsichtigte Änderungen dieser Liste durch Hinzufügung oder Ersetzung von Unterauftragsbearbeitern, so dass der für die Verarbeitung Verantwortliche die Möglichkeit hat, vor der Beauftragung des/der betreffenden Unterauftragsbearbeiter(s) Einspruch gegen diese Änderungen einzulegen. Ein solcher Einspruch darf nicht unangemessen erhoben werden. Die Parteien halten die Liste auf dem neuesten Stand.

b) Beauftragt der Auftragsbearbeiter einen Unterauftragsbearbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des für die Verarbeitung Verantwortlichen), so erfolgt dies im Rahmen eines Vertrags, der dem Unterauftragsbearbeiter dieselben Pflichten auferlegt wie dem Auftragsbearbeiter gemäss dieses ADV. Der Auftragsbearbeiter stellt sicher, dass der Unterauftragsbearbeiter die Verpflichtungen einhält, denen der Auftragsbearbeiter gemäss dieses ADV, Art. 28 Abs. 2 bis 4 der DSGVO und Art. 9 Abs. 3 DSG unterliegt.

c) Der Auftragsbearbeiter legt dem für die Verarbeitung Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Unterauftragsbearbeitungsvereinbarung und späterer Änderungen vor.

d) Der Auftragsbearbeiter bleibt gegenüber dem für die Verarbeitung Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsberarbeiters aus seinem Vertrag mit dem Auftragsbearbeiter verantwortlich. Der Auftragsbearbeiter meldet dem für die Verarbeitung Verantwortlichen, wenn der Unterauftragsberarbeiter seinen Verpflichtungen aus diesem Vertrag nicht nachkommt.

5.7 Internationale Übermittlungen

a) Jegliche Übermittlung von Personendaten in ein "Drittland" (jedes Land ausserhalb der EU/des EWR und der Schweiz) oder an eine internationale Organisation durch den Auftragsbearbeiter darf nur erfolgen, wenn sie gemäss Abschnitt A genehmigt wurde, und muss in Übereinstimmung mit Kapitel V der DSGVO und Abschnitt 2 des DSG erfolgen, soweit anwendbar.

b) Der für die Verarbeitung Verantwortliche erklärt sich damit einverstanden, dass, wenn der Auftragsbearbeiter einen Unterauftragsbearbeiter gemäss Klausel 5.6 mit der Durchführung bestimmter Bearbeitungstätigkeiten (im Auftrag des für die Verarbeitung Verantwortlichen) in einem Drittland beauftragt und diese Bearbeitungstätigkeiten die Übermittlung von Personendaten im Sinne der DSGVO bzw. des DSG beinhalten, der Auftragsbearbeiter und der Unterauftragsbearbeiter Standardvertragsklauseln verwenden können, die von der EU-Kommission auf der Grundlage von Artikel 46 Absatz 2 der DSGVO angenommen wurden, um die Anforderungen von Kapitel V der DSGVO zu erfüllen, sofern die Bedingungen für die Verwendung dieser Klauseln erfüllt sind und eine interne Bewertung zu dem Ergebnis geführt hat, dass eine solche Übermittlung dem Datenschutzniveau der DSGVO und des DSG entspricht.

6. Rechte der betroffenen Person

a) Der Auftragsbearbeiter unterrichtet den für die Verarbeitung Verantwortlichen unverzüglich über alle direkt von der betroffenen Person gestellten Anträge. Er antwortet nicht selbst auf diese Anfrage, es sei denn, er wurde von dem für die Verarbeitung Verantwortlichen dazu ermächtigt.

b) Der Auftragsbearbeiter unterstützt den für die Datenverarbeitung Verantwortlichen bei der Erfüllung seiner Verpflichtungen, auf die Anträge der betroffenen Personen auf Ausübung ihrer Rechte gemäss Kapitel III der DSGVO und Kapitel IV des DSG zu reagieren, und zwar

1. das Recht, informiert zu werden, wenn Personendaten von der betroffenen Person erhoben werden,
2. das Recht, informiert zu werden, wenn Personendaten nicht von der betroffenen Person erhalten wurden,
3. das Recht auf Auskunft durch die betroffene Person,
4. das Recht auf Berichtigung,
5. das Recht auf Löschung (“das Recht auf Vergessenwerden”),
6. das Recht auf Einschränkung der Verarbeitung,
7. die Meldepflicht zur Berichtigung oder Löschung von Personendaten oder zur Einschränkung der Verarbeitung,
8. das Recht auf Datenübertragbarkeit,
9. das Recht, Einspruch zu erheben,
10. das Recht, keiner Entscheidung unterworfen zu werden, die ausschliesslich auf einer automatisierten Verarbeitung, einschliesslich Profiling, beruht,
11. das Recht, die Einwilligung zu widerrufen.

c) Der Auftragsbearbeiter unterstützt den für die Verarbeitung Verantwortlichen, wenn eine betroffene Person bei der zuständigen Aufsichtsbehörde eine Beschwerde eingereicht hat, die Daten betrifft, die auf der Grundlage dieses ADV verarbeitet werden.

d) Zusätzlich zu der Verpflichtung des Auftragsbearbeiter, den für die Verarbeitung Verantwortlichen gemäss Artikel 6 Buchstabe b zu unterstützen, unterstützt der Auftragsbearbeiter den für die Verarbeitung Verantwortlichen bei der Einhaltung der folgenden Verpflichtungen, wobei die Art der Verarbeitung und die dem Auftragsbearbeiter zur Verfügung stehenden Informationen berücksichtigt werden:

1. Die Verpflichtung, eine Verletzung des Schutzes von Personendaten unverzüglich nach Bekanntwerden der zuständigen Aufsichtsbehörde mitzuteilen (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen), in Übereinstimmung mit Art. 33 der Datenschutz-Grundverordnung und Art. 24 Abs. 1-3 des DSG;

2. die Verpflichtung, der betroffenen Person die Verletzung des Schutzes von Personendaten unverzüglich mitzuteilen, wenn die Verletzung des Schutzes personenbezogener Daten

wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, gemäss Art. 34 der DSGVO und Art. 24 Abs. 3 des DSG;

3. die Verpflichtung zur Durchführung einer Abschätzung der Folgen der geplanten Verarbeitungen für den Schutz von Personendaten (eine "Datenschutz-Folgenabschätzung"), wenn eine Art der Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, gemäss Art. 35 der DSGVO und Art. 22 des DSG;

4. die Verpflichtung, die zuständige Aufsichtsbehörde vor der Verarbeitung zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn der für die Verarbeitung Verantwortliche keine Massnahmen zur Risikominderung ergreift, gemäss Art. 36 der DSGVO und Art. 23 des DSG.

e) Die Vertragsparteien legen in Abschnitt C die geeigneten technischen und organisatorischen Massnahmen fest, durch die der Auftragsbearbeiter den für die Verarbeitung Verantwortlichen bei der Anwendung dieser Klausel zu unterstützen hat, sowie den Umfang und das Ausmass der erforderlichen Unterstützung.

7. Meldung von Verletzungen des Schutzes von Personendaten

a) Im Falle einer Verletzung des Schutzes von Personendaten arbeitet der Auftragsbearbeiter nach Treu und Glauben mit dem für die Verarbeitung Verantwortlichen zusammen und unterstützt ihn in jeder Weise, die für den für die Verarbeitung Verantwortlichen erforderlich ist, um seinen Verpflichtungen gemäss Artikel 33 und 34 DSGVO und Artikel 24 DSG nachzukommen, wobei die Art der Verarbeitung und die dem Auftragsbearbeiter zur Verfügung stehenden Informationen berücksichtigt werden.

b) Der Auftragsbearbeiter unterstützt den für die Verarbeitung Verantwortlichen bei der Meldung der Verletzung des Schutzes von Personendaten an die zuständige Aufsichtsbehörde, sofern zutreffend. Der Auftragsbearbeiter ist verpflichtet, insbesondere bei der Beschaffung der folgenden Informationen behilflich zu sein, die gemäss Artikel 33 Absatz 3 der DSGVO bzw. Artikel 24 Absatz 2 des DSG in der Meldung des für die Verarbeitung Verantwortlichen angegeben werden müssen:

1. Die Art der Personendaten, einschliesslich, soweit möglich, die Kategorien und die ungefähre Anzahl der betroffenen Personen sowie die Kategorien und die ungefähre Anzahl der betroffenen personenbezogenen Datensätze;
2. die wahrscheinlichen Folgen der Verletzung des Schutzes von Personendaten;
3. die Massnahmen, die der für die Verarbeitung Verantwortliche ergriffen hat oder zu ergreifen gedenkt, um die Verletzung des Schutzes personenbezogener Daten zu beheben, gegebenenfalls einschliesslich Massnahmen zur Abschwächung möglicher negativer Auswirkungen.

8. Beendigung

a) Unbeschadet der Bestimmungen der DSGVO bzw. des DSG kann der für die Verarbeitung Verantwortliche den Auftragsbearbeiter anweisen, die Verarbeitung von Personendaten vorübergehend einzustellen, bis dieser diesen ADV einhält oder der Vertrag gekündigt wird, falls der Auftragsbearbeiter gegen seine Verpflichtungen aus diesem ADV verstösst. Der Auftragsbearbeiter unterrichtet den für die Verarbeitung Verantwortlichen unverzüglich, falls er aus irgendeinem Grund nicht in der Lage ist, diesen ADV einzuhalten.

b) Der für die Verarbeitung Verantwortliche ist berechtigt, diesen ADV zu kündigen, wenn:

1. Die Verarbeitung personenbezogener Daten durch den Auftragsbearbeiter von dem für die Verarbeitung Verantwortlichen gemäss Buchstabe a vorübergehend ausgesetzt wurde, der Verstoss des Auftragsbearbeiter erheblich ist und die Einhaltung dieses ADV nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats, wiederhergestellt wird;

2. Der Auftragsbearbeiter verstösst in erheblichem Masse oder dauerhaft gegen diesen ADV oder gegen seine Verpflichtungen nach der DSGVO bzw. dem DSG, und es ist nicht zu erwarten, dass dieser Verstoss behoben wird;

3. Der Auftragsbearbeiter einer verbindlichen Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde in Bezug auf seine Verpflichtungen aus diesem ADV oder aus der DSGVO bzw. dem DSG nicht nachkommt.

c) Diese Vereinbarung bleibt in vollem Umfang in Kraft, solange die Basisvereinbarung in Kraft bleibt. Alle Bestimmungen dieses ADV, die ausdrücklich oder stillschweigend bei oder nach Beendigung des Basisvertrags zum Schutz von Personendaten in Kraft treten oder fortbestehen sollen, bleiben in vollem Umfang in Kraft.

9. Haftung und Schadloshaltung

Die Haftung beider Parteien aus diesem oder in Zusammenhang mit diesem unterstehen den Haftungsbeschränkungen und -ausschlüssen des Basisvertrags.

Abschnitt C – TOMs

Beschreibung der technischen und organisatorischen Massnahmen, die von dem/den Auftragsbearbeiter(n) durchgeführt werden:

1. Organisatorische Sicherheitsmassnahmen

1.1 Sicherheitsmanagement

a) Sicherheitskonzept und -verfahren: Der Auftragsbearbeiter verfügt über ein dokumentiertes Sicherheitskonzept für die Verarbeitung von Personendaten.

b) Rollen und Verantwortlichkeiten:

1. Die Rollen und Verantwortlichkeiten im Zusammenhang mit der Verarbeitung von Personendaten sind klar definiert und im Einklang mit dem Sicherheitskonzept zugewiesen.

2. Bei internen Umstrukturierungen oder Kündigungen und beim Wechsel des Arbeitsplatzes ist der Widerruf von Rechten und Zuständigkeiten mit entsprechenden Übergabeverfahren klar definiert.

c) Politik der Zugangskontrolle: Jeder Rolle, die an der Verarbeitung von Personendaten beteiligt ist, werden nach dem Need-to-know-Prinzip spezifische Zugriffskontrollrechte zugewiesen.

d) Verwaltung der Ressourcen/Vermögenswerte: Der Auftragsbearbeiter verfügt über ein Register der für die Verarbeitung von Personendaten verwendeten IT-Ressourcen (Hardware, Software und Netzwerk). Eine bestimmte Person ist mit der Pflege und Aktualisierung des Registers betraut (z.B. der IT-Beauftragte).

e) Änderungsmanagement: Der Auftragsbearbeiter stellt sicher, dass alle Änderungen am IT-System von einer bestimmten Person (z. B. dem IT- oder Sicherheitsbeauftragten) registriert und überwacht werden. Dieser Prozess wird regelmässig überwacht.

1.2 Reaktion auf Zwischenfälle und Geschäftskontinuität

a) Umgang mit Zwischenfällen / Verletzungen des Schutzes von Personendaten:

1. Es wird ein Plan für die Reaktion auf Zwischenfälle mit detaillierten Verfahren festgelegt, um eine wirksame und ordnungsgemässe Reaktion auf Zwischenfälle im Zusammenhang mit Personendaten zu gewährleisten.

2. Der Auftragsbearbeiter meldet dem für die Verarbeitung Verantwortlichen unverzüglich jeden Sicherheitsvorfall, der zu einem Verlust, einem Missbrauch oder einer unbefugten Kenntnisnahme von Personendaten geführt hat.

b) Geschäftskontinuität: Der Auftragsbearbeiter hat die wichtigsten Verfahren und Kontrollen festgelegt, die zu befolgen sind, um das erforderliche Mass an Kontinuität und Verfügbarkeit des IT-Systems zur Verarbeitung von Personendaten (im Falle eines Zwischenfalls/einer Verletzung des Schutzes von Personendaten) zu gewährleisten.

1.3 HR

a) Vertraulichkeit des Personals: Der Auftragsbearbeiter stellt sicher, dass alle Mitarbeiter ihre Verantwortlichkeiten und Pflichten im Zusammenhang mit der Verarbeitung von Personendaten kennen. Die Rollen und Zuständigkeiten werden während des Verfahrens vor der Einstellung und/oder bei der Einarbeitung klar kommuniziert.

b) Schulung: Der Auftragsbearbeiter stellt sicher, dass alle Mitarbeiter angemessen über die Sicherheitskontrollen des IT-Systems informiert sind, die sich auf ihre tägliche Arbeit beziehen. Die mit der Verarbeitung von Personendaten befassten Mitarbeiter werden durch regelmässige Sensibilisierungskampagnen auch angemessen über die einschlägigen Datenschutzanforderungen und rechtlichen Verpflichtungen informiert.

2. Technische Sicherheitsmassnahmen

2.1 Zugangskontrolle und Authentifizierung

a) Ein Zugangskontrollsystem, das für alle Benutzer, die auf das IT-System zugreifen, gilt, wurde eingeführt. Das System ermöglicht das Anlegen, Genehmigen, Überprüfen und Löschen von

Benutzerkonten.

b) Die Verwendung von gemeinsamen Benutzerkonten wird vermieden. In Fällen, in denen dies notwendig ist, wird sichergestellt, dass alle Benutzer des gemeinsamen Kontos die gleichen Rollen und Verantwortlichkeiten haben.

c) Bei der Gewährung des Zugangs oder der Zuweisung von Nutzerrollen ist der Grundsatz “Need-To-Know” zu beachten, um die Zahl der Nutzer, die Zugang zu Personendaten haben, auf diejenigen zu beschränken, die diesen Zugang für die Erfüllung der Verarbeitungszwecke des Auftragsbearbeiter benötigen.

d) Wenn die Authentifizierungsmechanismen auf Passwörtern beruhen, verlangt der Auftragsbearbeiter Zwei-Faktor-Identifizierung.

e) Die Authentifizierungsdaten (z. B. Benutzer-ID und Passwort) dürfen niemals ungeschützt über das Netz übertragen werden.

2.2 Protokollierung und Überwachung

Für jedes System/jede Anwendung, das/die für die Verarbeitung von Personendaten verwendet wird, werden Protokolldateien aktiviert, wo technisch möglich und umsetzbar. Sie umfassen, wo technisch möglich und umsetzbar, alle Arten des Zugriffs auf Daten (Ansicht, Änderung, Löschung).

2.3 Sicherheit von Daten im Ruhezustand

a) Server/Databank-Sicherheit

1. Datenbank- und Anwendungsserver sind so konfiguriert, dass sie unter einem separaten Konto mit minimalen Betriebssystemprivilegien laufen, um korrekt zu funktionieren.

2. Datenbank- und Anwendungsserver verarbeiten nur die Personendaten, deren Bearbeitung zur Erreichung des Verarbeitungszwecks tatsächlich erforderlich ist.

2. Netz-/Kommunikationssicherheit

a) Bei jedem Zugriff über das Internet wird die Kommunikation durch kryptographische Protokolle verschlüsselt.

b) Der Verkehr zum und vom IT-System wird durch Firewalls und Intrusion Detection Systeme überwacht und kontrolliert.

2.5 Backups

a) Sicherungs- und Datenwiederherstellungsverfahren sind definiert, dokumentiert und klar mit Rollen und Verantwortlichkeiten verknüpft.

b) Backups werden in angemessenem Umfang physisch und ökologisch geschützt, entsprechend den Standards, die für die ursprünglichen Daten gelten.

c) Die Ausführung der Backups wird auf Vollständigkeit überwacht.

2.6 Mobile/tragbare Geräte

a) Es werden Verfahren für die Verwaltung mobiler und tragbarer Geräte festgelegt und dokumentiert, die klare Regeln für deren ordnungsgemässe Verwendung enthalten.

b) Mobile Geräte, die auf das Informationssystem zugreifen dürfen, werden vorab registriert und autorisiert.

2.7 Sicherheit im Lebenszyklus von Anwendungen

Während des Entwicklungszyklus werden bewährte Praktiken, der neueste Stand der Technik und anerkannte sichere Entwicklungsverfahren oder -standards befolgt.

2.8 Löschung/Entsorgung von Daten

a)Die Datenträger werden vor ihrer Entsorgung mit Software überschrieben. In Fällen, in denen dies nicht möglich ist (CDs, DVDs usw.), werden sie physisch vernichtet.

b) Papier und tragbare Datenträger, die zur Speicherung personenbezogener Daten verwendet werden, werden vernichtet.

2.9 Physische Sicherheit

Die physische Umgebung der IT-Systeminfrastruktur ist für nicht autorisiertes Personal nicht zugänglich. Durch geeignete technische Massnahmen (z.B. Einbruchmeldeanlage, chipkartengesteuertes Drehkreuz, Ein-Personen-Sicherheitszugangssystem, Schliessanlage) oder organisatorische Massnahmen (z.B. Wachdienst) sind die Sicherheitsbereiche und deren Zugänge gegen das Betreten durch Unbefugte zu schützen.

Unterschriften

Verantwortlicher

Datum:

Name:

Unterschrift:

Auftragsbearbeiter

Datum:

Name:

Kontera GmbH

Unterschrift:
