Standardvertragsklauseln

Für die Zwecke von Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 (DSGVO)

Der Kunde
(der "**Datenverantwortliche**")

und

SameSystem A/S
CVR-/VAT-Nr.: 31487927
Rentemestervej 2A
2400 Kopenhagen NV
Dänemark
(der "**Datenverarbeiter**")

jeder einzelne eine "Partei"; zusammen die "Parteien"

HABEN die folgenden Vertragsklauseln (die Klauseln) VEREINBART, um die Anforderungen der DSGVO zu erfüllen und den Schutz der Rechte der betroffenen Person zu gewährleisten. Diese Klauseln sind Teil des Lizenzvertrags zwischen den Parteien.

Diese Klauseln gelten für alle Verarbeitungen personenbezogener Daten, die vom Datenverarbeiter (einschließlich seiner Tochtergesellschaften) im Auftrag des Datenverantwortlichen (einschließlich seiner Tochtergesellschaften) durchgeführt werden.

1. Inhaltsverzeichnis

2. Präambel

1. Diese Vertragsklauseln (die Klauseln) legen die Rechte und Pflichten des Datenverantwortlichen und des Datenverarbeiters bei der Verarbeitung personenbezogener Daten im Auftrag des Datenverantwortlichen fest.

2. Die Klauseln wurden entwickelt, um die Einhaltung von Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) durch die Parteien sicherzustellen.

3. Der Datenverarbeiter erbringt die im Lizenzvertrag und in den allgemeinen Lizenzbedingungen zwischen den Parteien beschriebenen Dienstleistungen und verarbeitet zur Erfüllung des Lizenzvertrags personenbezogene Daten im Auftrag des für die Datenverarbeitung Verantwortlichen in Übereinstimmung mit den Klauseln.

4. Diese Vereinbarung über die Datenverarbeitung ersetzt alle früheren Vereinbarungen über die Datenverarbeitung zwischen dem Datenverarbeiter und dem für die Datenverarbeitung Verantwortlichen.

5. Vier Anhänge sind den Klauseln beigefügt und bilden einen integralen Bestandteil der Klauseln.

6. Anhang A enthält Einzelheiten über die Verarbeitung personenbezogener Daten, einschließlich des Zwecks und der Art der Verarbeitung, der Art der personenbezogenen Daten, der Kategorien der betroffenen Personen und der Dauer der Verarbeitung.

7. Anhang B enthält die Bedingungen des Datenverantwortlichen für den Einsatz von Unterauftragsverarbeitern und eine Liste der vom Datenverantwortlichen zugelassenen Unterauftragsverarbeiter.

8. Anhang C enthält die Anweisungen des Datenverantwortlichen in Bezug auf die Verarbeitung personenbezogener Daten, die vom Datenverarbeiter umzusetzenden Mindestsicherheitsmaßnahmen und die Art und Weise, wie Audits des Datenverarbeiters und etwaiger Unterauftragsverarbeiter durchgeführt werden sollen.

9. Anhang D enthält Bestimmungen für andere Tätigkeiten, die nicht von den Klauseln erfasst werden.

10. Die Klauseln und ihre Anhänge sind von beiden Parteien schriftlich, auch elektronisch, aufzubewahren.

11. Die Klauseln befreien den Datenverarbeiter nicht von Verpflichtungen, denen er gemäß der Allgemeinen Datenschutzverordnung (DSGVO) oder anderen Rechtsvorschriften unterliegt.

3. Die Rechte und Pflichten des Datenverantwortlichen

1. Der Datenverantwortlichen ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO (siehe Artikel 24 DSGVO), den geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten[1] und den Klauseln erfolgt.

2. Der Datenverantwortlichen hat das Recht und die Pflicht, Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu treffen.

3. Der Datenverantwortlichen ist u. a. dafür verantwortlich, dass die Verarbeitung personenbezogener Daten, mit welcher der Datenverarbeiter beauftragt wird, auf einer Rechtsgrundlage beruht.

4. Der Datenverarbeiter handelt gemäß den Anweisungen

1. Der Datenverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Datenverantwortlichen verarbeiten, es sei denn, er ist aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen er unterliegt, dazu verpflichtet. Der Datenverantwortlichen kann während der gesamten Dauer der Verarbeitung personenbezogener Daten auch nachträgliche Weisungen erteilen; diese Weisungen sind jedoch stets zu dokumentieren und schriftlich, auch elektronisch, in Verbindung mit den Klauseln aufzubewahren.

2. Der Datenverarbeiter informiert den Datenverantwortlichen unverzüglich, wenn die Anweisungen des Datenverantwortlichen nach Ansicht des Datenverarbeiters gegen die DSGVO oder die geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstoßen.

5. Vertraulichkeit

1. Der Datenverarbeiter gewährt Zugang zu den personenbezogenen Daten, die im Auftrag des Datenverantwortlichen verarbeitet werden, nur den ihm unterstellten Personen, die sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen, und nur auf der Grundlage der Notwendigkeit der Kenntnisnahme. Die Liste der Personen, denen Zugang gewährt wurde, wird regelmäßig überprüft. Auf der Grundlage dieser Überprüfung kann der Zugang zu personenbezogenen Daten widerrufen werden, wenn er nicht mehr erforderlich ist, und die personenbezogenen Daten sind dann für diese Personen nicht mehr zugänglich.

2. Der Datenverarbeiter weist auf Verlangen des Datenverantwortlichen nach, dass die betroffenen Personen, die dem Datenverarbeiter unterstellt sind, der oben genannten Geheimhaltungspflicht unterliegen.

6. Sicherheit der Verarbeitung

1. Artikel 32 DSGVO sieht vor, dass der Datenverantwortlichen und der Datenverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte

[1] Die in den Klauseln enthaltenen Verweise auf "Mitgliedstaaten" sind als Verweise auf "EWR-Mitgliedstaaten" zu verstehen.

und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Maß an Sicherheit zu gewährleisten.

Der Datenverantwortlichen bewertet die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen und ergreift Maßnahmen, um diese Risiken zu mindern. Je nach Relevanz können die Maßnahmen Folgendes umfassen:

a. Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;

b. die Fähigkeit, die ständige Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste zu gewährleisten;

c. die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen;

d. ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

2. Gemäß Artikel 32 DSGVO muss der Datenverarbeiter auch - unabhängig von dem Datenverantwortlichen - die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bewerten und Maßnahmen zur Minderung dieser Risiken ergreifen. Zu diesem Zweck stellt der Datenverantwortlichen dem Datenverarbeiter alle Informationen zur Verfügung, die zur Ermittlung und Bewertung dieser Risiken erforderlich sind.

3. Darüber hinaus unterstützt der Datenverarbeiter den Datenverantwortlichen bei der Einhaltung seiner Pflichten gemäß Artikel 32 DSGVO, indem er dem Datenverantwortlichen *unter anderem* Informationen über die technischen und organisatorischen Maßnahmen zur Verfügung stellt, die der Datenverarbeiter gemäß Artikel 32 DSGVO bereits umgesetzt hat, sowie alle anderen Informationen, die der Datenverantwortlichen benötigt, um seinen Pflichten gemäß Artikel 32 DSGVO nachzukommen.

   Erfordert die weitere Minderung der festgestellten Risiken nach Einschätzung des Datenverantwortlichen zusätzliche, vom Datenverarbeiter zu ergreifende Maßnahmen, die über die, die der Datenverarbeiter gemäß Artikel 32 DSGVO bereits ergriffen hat, hinausgehen, so führt der Datenverantwortlichen diese zusätzlichen Maßnahmen in Anhang C auf.

7. Einsatz von Unterauftragsverarbeitern

1. Der Datenverarbeiter muss die in Artikel 28 Absätze 2 und 4 DSGVO genannten Anforderungen erfüllen, um einen anderen Datenverarbeiter (einen Unterauftragsverarbeiter) zu beauftragen.

2. Der Datenverarbeiter darf daher ohne vorherige allgemeine schriftliche Genehmigung des Datenverantwortlichen keinen anderen Verarbeiter (Unterauftragsverarbeiter) mit der Erfüllung der Klauseln beauftragen.

3. Der Datenverantwortliche erteilt dem Datenverarbeiter die allgemeine Genehmigung für die Beauftragung von Unterauftragsverarbeitern. Der Datenverarbeiter unterrichtet

den Datenverantwortlichen mindestens 30 Tage im Voraus schriftlich über alle beabsichtigten Änderungen in Bezug auf das Hinzufügen oder den Austausch von Unterauftragsverarbeitern, so dass der Datenverantwortliche die Möglichkeit hat, vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter(s) Einwände gegen diese Änderungen zu erheben. Längere Vorankündigungsfristen für bestimmte Unterauftragsverarbeitungsdienste können in Anlage B angegeben werden. Die Liste der vom Datenverantwortlichen bereits genehmigten Unterauftragsverarbeiter findet sich in Anhang B.

4. Beauftragt der Datenverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Datenverantwortlichen, so werden diesem Unterauftragsverarbeiter durch einen Vertrag oder einen anderen Rechtsakt nach EU-Recht oder dem Recht eines Mitgliedstaats dieselben Datenschutzverpflichtungen auferlegt, wie sie in den Klauseln festgelegt sind, insbesondere die Bereitstellung ausreichender Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen in einer Weise, dass die Verarbeitung den Anforderungen der Klauseln und der DSGVO entspricht.

   Der Datenverarbeiter ist daher dafür verantwortlich, vom Unterauftragsverarbeiter einzufordern, zumindest die Verpflichtungen einzuhalten, denen der Datenverarbeiter gemäß den Klauseln und der DSGVO unterliegt.

5. Eine Kopie eines solchen Unterauftragsverarbeitungsvertrags und spätere Änderungen sind - auf Verlangen des Datenverantwortlichen - dem für Datenverantwortlichen vorzulegen, so dass der Datenverantwortliche die Möglichkeit hat, sicherzustellen, dass dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt werden, wie sie in den Klauseln festgelegt sind. Klauseln zu geschäftsbezogenen Fragen, die den datenschutzrechtlichen Inhalt der Unterauftragsverarbeitungsvereinbarung nicht berühren, müssen dem Datenverantwortlichen nicht vorgelegt werden.

6. Kommt der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, so bleibt der Datenverarbeiter gegenüber dem Datenverantwortlichen in Bezug auf die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters in vollem Umfang haftbar. Dies berührt nicht die Rechte der betroffenen Personen nach der Datenschutz-Grundverordnung - insbesondere die in den Artikeln 79 und 82 der Datenschutz-Grundverordnung vorgesehenen - gegenüber dem Datenverantwortlichen und dem Datenverarbeiter, einschließlich des Unterauftragsverarbeiters.

8. Übermittlung von Daten an Drittländer oder internationale Organisationen

1. Jegliche Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen durch den Datenverarbeiter darf nur auf der Grundlage dokumentierter Anweisungen des Datenverantwortlichen erfolgen und muss stets im Einklang mit Kapitel V der Datenschutz-Grundverordnung stehen.

2. Ist die Übermittlung von Daten an Drittländer oder internationale Organisationen, mit welcher der Datenverarbeiter nicht vom Datenverantwortlichen beauftragt wurde, nach dem Recht der EU oder eines Mitgliedstaats, dem der Datenverarbeiter unterliegt, erforderlich, so unterrichtet der Datenverarbeiter den Datenverantwortlichen vor der Verarbeitung über diese rechtliche Anforderung, es sei denn, das betreffende Recht verbietet eine solche Unterrichtung aus wichtigen Gründen des öffentlichen Interesses.

3. Ohne dokumentierte Anweisungen des Datenverantwortlichen kann der Datenverarbeiter daher im Rahmen der Klauseln nicht:

    a. personenbezogene Daten an einen Datenverantwortlichen oder einen Datenverarbeiter in einem Drittland oder in einer internationalen Organisation übermitteln

    b. die Verarbeitung personenbezogener Daten an einen Unterauftragsverarbeiter in einem Drittland übertragen

    c. die Verarbeitung der personenbezogenen Daten durch den Datenverarbeiter in einem Drittland veranlassen

4. Die Anweisungen des Datenverantwortlichen für die Übermittlung personenbezogener Daten in ein Drittland, gegebenenfalls einschließlich des Übermittlungsinstruments gemäß Kapitel V DSGVO, auf das sie sich stützen, sind in Anhang C.6 aufgeführt.

5. Die Klauseln sind nicht mit den Standard-Datenschutzklauseln im Sinne von Artikel 46 Absatz 2 Buchstaben c und d DSGVO zu verwechseln, und die Klauseln können von den Parteien nicht als Übermittlungsinstrument gemäß Kapitel V der DSGVO herangezogen werden.

9. Unterstützung für den Datenverantwortlichen

1. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Datenverarbeiter den Datenverantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Verpflichtungen des Datenverantwortlichen zur Beantwortung von Anträgen auf Ausübung der Rechte der betroffenen Person gemäß Kapitel III DSGVO.

    Dies bedeutet, dass der Datenverarbeiter den Datenverantwortlichen, soweit dies möglich ist, unterstützen muss bei der Einhaltung der Vorschriften in Bezug auf:

    a. das Recht, bei der Erhebung personenbezogener Daten der betroffenen Person informiert zu werden
    b. das Recht, informiert zu werden, wenn personenbezogene Daten nicht von der betroffenen Person erhalten worden sind
    c. das Recht auf Auskunft durch die betroffene Person
    d. das Recht auf Berichtigung
    e. das Recht auf Löschung ("das Recht auf Vergessenwerden")
    f. das Recht auf Einschränkung der Verarbeitung
    g. Meldepflicht zur Berichtigung oder Löschung personenbezogener Daten oder zur Einschränkung der Verarbeitung
    h. das Recht auf Datenübertragbarkeit
    i. das Recht auf Widerspruch
    j. das Recht, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht

2. Zusätzlich zu der Verpflichtung des Datenverarbeiters, den Datenverantwortlichen gemäß Ziffer 6.3. zu unterstützen, muss der Datenverarbeiter den Datenverantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen bei der Einhaltung der Vorschriften in Bezug auf:

    a. Die Verpflichtung des Datenverantwortlichen, die Verletzung des Schutzes personenbezogener Daten unverzüglich und nach Möglichkeit spätestens 72 Stunden, nachdem er davon Kenntnis erlangt hat, der zuständigen Aufsichtsbehörde, der dänischen Datenschutzbehörde (Datatilsynet), zu melden, es sei denn, die Verletzung des Schutzes personenbezogener Daten wird wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen;

    b. die Verpflichtung des Datenverantwortlichen, der betroffenen Person die Verletzung des Schutzes personenbezogener Daten unverzüglich mitzuteilen, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt;

    c. die Verpflichtung des Datenverantwortlichen, eine Bewertung der Auswirkungen der geplanten Verarbeitungen auf den Schutz personenbezogener Daten vorzunehmen (Datenschutz-Folgenabschätzung);

    d. die Verpflichtung des Datenverantwortlichen, die zuständige Aufsichtsbehörde, die dänische Datenschutzbehörde (Datatilsynet), vor der Verarbeitung zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko mit sich bringen würde, wenn der Datenverantwortliche keine Maßnahmen zur Risikominderung ergreift.

3. Die Parteien legen in Anlage C die geeigneten technischen und organisatorischen Maßnahmen fest, mit denen der Datenverarbeiter den Datenverantwortlichen zu unterstützen hat, sowie den Umfang und das Ausmaß der erforderlichen Unterstützung. Dies gilt für die in den Ziffern 9.1. und 9.2. vorgesehenen Verpflichtungen.

10. Benachrichtigung über die Verletzung des Schutzes personenbezogener Daten

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Datenverarbeiter den Datenverantwortlichen ohne unangemessene Verzögerung, nachdem er davon Kenntnis erlangt hat.

2. Die Benachrichtigung des Datenverarbeiters an den Datenverantwortlichen erfolgt nach Möglichkeit innerhalb von 24 Stunden, nachdem der Datenverarbeiter von der Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat, damit der Datenverantwortliche seiner Verpflichtung nachkommen kann, die Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden, vgl. Artikel 33 DSGVO.

3. Gemäß Klausel 9 Absatz 2 Buchstabe a unterstützt der Datenverarbeiter den Datenverantwortlichen bei der Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, was bedeutet, dass der Datenverarbeiter bei der Beschaffung der nachstehend aufgeführten Informationen behilflich ist, die

gemäß Artikel 33 Absatz 3 DSGVO in der Meldung des Datenverantwortlichen an die zuständige Aufsichtsbehörde angegeben werden müssen:

a. die Art der personenbezogenen Daten, einschließlich, soweit möglich, die Kategorien und die ungefähre Anzahl der betroffenen Personen sowie die Kategorien und die ungefähre Anzahl der betroffenen personenbezogenen Datensätze;

b. die voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

c. die Maßnahmen, die der Datenverantwortliche ergriffen hat oder zu ergreifen gedenkt, um die Verletzung des Schutzes personenbezogener Daten zu beheben, gegebenenfalls einschließlich Maßnahmen zur Abschwächung möglicher nachteiliger Auswirkungen.

4. Die Parteien legen in Anhang C alle Angaben fest, die der Datenverarbeiter bei der Unterstützung des Datenverantwortlichen bei der Meldung einer Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu machen hat.

11. Löschung und Rückgabe von Daten

1. Bei Beendigung der Erbringung von Dienstleistungen im Bereich der Verarbeitung personenbezogener Daten ist der Datenverarbeiter verpflichtet, alle im Auftrag des Datenverantwortlichen verarbeiteten personenbezogenen Daten zu löschen und/oder zurückzugeben und dem Datenverantwortlichen zu bestätigen, dass er dies getan hat, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten schreibt die Speicherung der personenbezogenen Daten vor.

12. Audit und Inspektion

1. Der Datenverarbeiter stellt dem Datenverantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Artikel 28 und in den Klauseln festgelegten Verpflichtungen nachzuweisen, und er gestattet Audits, einschließlich Inspektionen, die von dem Datenverantwortlichen oder einem anderen von dem Datenverantwortlichen beauftragten Prüfer durchgeführt werden, und leistet seinen Beitrag dazu.

2. Die Verfahren für Audits, einschließlich Inspektionen, des Datenverarbeiters und der Unterauftragsverarbeiter durch den Datenverantwortlichen sind in den Anhängen C.7. und C.8. aufgeführt.

3. Der Datenverarbeiter ist verpflichtet, den Aufsichtsbehörden, die gemäß den geltenden Rechtsvorschriften Zugang zu den Einrichtungen des Datenverantwortlichen und des Datenverarbeiters haben, oder den im Namen dieser Aufsichtsbehörden handelnden Vertretern gegen Vorlage eines entsprechenden Ausweises Zugang zu den physischen Einrichtungen des Datenverarbeiters zu gewähren.

13. Die Vereinbarung der Parteien über andere Bedingungen

1. Die Parteien können weitere Klauseln über die Erbringung des Dienstes zur Verarbeitung personenbezogener Daten vereinbaren, in denen z. B. die Haftung geregelt ist, sofern sie nicht direkt oder indirekt im Widerspruch zu den Klauseln stehen oder die Grundrechte und -freiheiten der betroffenen Person und den durch die DSGVO gewährten Schutz beeinträchtigen.

14. Beginn und Laufzeit

1. Die Klauseln treten mit dem Datum der Unterzeichnung der Lizenzvereinbarung durch beide Parteien in Kraft.

2. Beide Parteien haben das Recht, eine Neuverhandlung der Klauseln zu verlangen, wenn Gesetzesänderungen oder die Unzweckmäßigkeit der Klauseln Anlass zu einer solchen Neuverhandlung geben sollten.

3. Die Klauseln gelten für die Dauer der Erbringung von Dienstleistungen zur Verarbeitung personenbezogener Daten. Für die Dauer der Erbringung von Dienstleistungen zur Verarbeitung personenbezogener Daten können die Klauseln nicht gekündigt werden, es sei denn, die Parteien haben andere Klauseln für die Erbringung von Dienstleistungen zur Verarbeitung personenbezogener Daten vereinbart.

4. Wird die Erbringung von Dienstleistungen zur Verarbeitung personenbezogener Daten beendet und werden die personenbezogenen Daten gemäß Klausel 11.1. und Anhang C.4. gelöscht oder an den Datenverantwortlichen zurückgegeben, können die Klauseln von beiden Parteien durch schriftliche Mitteilung gekündigt werden.

15. Kontakt

Der für die Datenverarbeitung Verantwortliche kann den Datenverarbeiter kontaktieren unter: dataprivacy@samesystem.com für alle allgemeinen Anfragen zu diesen Klauseln sowie im Falle von Datenverstößen.

Anhang A) Informationen über die Verarbeitung

A.1. Der Zweck der Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen ist:

Dass der Datenverantwortliche das Online-Workforce-Management-System von SameSystem (SameSystem) einsetzen kann, um Informationen über seine Mitarbeiter zu sammeln und zu verarbeiten und seine Mitarbeiter zu verwalten.

A.2. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen bezieht sich hauptsächlich auf (die Art der Verarbeitung):

Der Datenverarbeiter stellt dem Datenverantwortlichen SameSystem zur Verfügung und speichert im Auftrag des Datenverantwortlichen personenbezogene Daten über die Mitarbeiter des Datenverantwortlichen auf den Servern des Datenverarbeiters und des zugelassenen Unterauftragsverarbeiters.

A.3. Die Verarbeitung umfasst die folgenden Arten personenbezogener Daten über betroffene Personen:

- Name
- Geburtsdatum
- Sozialversicherungsnummer/Nationale Versicherungsnummer
- E-Mail Adresse
- Telefon-Nummer
- Wohnanschrift
- Gehalt/Rente
- Gehaltsabrechnung und Mitarbeiternummer
- Berufliche Funktion
- Arbeitszeiten
- Abteilung
- Korrespondenz zwischen betroffenen Personen
- Abwesenheit und Urlaub (inkl. Elternzeit und Abwesenheit aufgrund von Urlaub und Krankheit, ohne ärztliche Atteste)
- Verwarnungen/Entlassungen
- Leistungen
- Andere Funktionen/Verantwortlichkeiten Alle personenbezogenen Daten, zu denen der Datenverarbeiter Zugang erhält, sind vertraulich zu behandeln.

A.4. Die Verarbeitung umfasst die folgenden Kategorien von betroffenen Personen:

- Mitarbeiter des Datenverantwortlichen.

A.5. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen kann bei Inkrafttreten der Klauseln erfolgen. Die Bearbeitung hat folgende Dauer:

Die Klauseln bleiben bis zur Beendigung der Lizenzvereinbarung in Kraft und enden gemäß Klausel 14 oben.

Anhang B) Zugelassene Unterauftragsverarbeiter

B.1. Genehmigte Unterauftragsverarbeiter

Mit Inkrafttreten der Klauseln genehmigt der Datenverantwortliche die Beauftragung der folgenden Unterauftragsverarbeiter:

NAME	GASTGEBERLAND	ADRESSE INKL. LAND	BESCHREIBUNG DER VERARBEITUNG
SameSystemUAB , LT100004691219	Keine Datenspeicherung	Didžioji g. 25, LT-01130, Vilnius, Litauen	Entwicklung und Verbesserung des IT-Systems. Technische Hilfe, falls erforderlich.
Hetzner OnlineGmbH , DE812871812	Deutschland (Hauptstandort) und Finnland (Backup-Standort)	Industrie str. 25, 91710 Gunzenhausen, Deutschland	Die Speicherung aller Daten im System, einschließlich personenbezogener Daten.
Scaleway SAS	Frankreich	8 rue de la Ville l'Evêque, 75008 Paris, France	Die Speicherung von Daten in Frankreich. Dies betrifft in erster Linie Sicherungsdaten.
Link Mobility Gruppe	Norwegen	Langkaia 1 - Havnelageret, 0150, Oslo, Norwegen	Zustellung von SMS. (Es werden keine Daten in den USA verarbeitet)
SMTP.DK ApS	Dänemark	Refshalevej 163A, 1. Tv 1432 København K, Dänemark	Zustellung von E-Mails.
E-Signatur DanmarkA/S CVR. 38491687	Irland	Lersø Park Alle 107, 2100 Kopenhagen Ø. Dänemark	Digitale Signaturen
Sendbird, Inc	Deutschland	400 1st Ave San Mateo, California 94401 United States	Interne Chat- und Messaging-Funktionalität innerhalb der SameSystem-Lösung (Chat zwischen den Benutzern). Es werden nur der 'Anzeigename' des Benutzers und die Chats/Nachrichten verarbeitet. NB: Dies ist ein optionaler Service, den der Kunde auf Wunsch von SameSystem aktivieren lassen kann.

Der Datenverantwortliche genehmigt bei Inkrafttreten der Klauseln den Einsatz der oben genannten Unterauftragsverarbeiter für die beschriebene Verarbeitung für diese Partei. Der Datenverarbeiter ist nicht berechtigt, ohne die ausdrückliche schriftliche Genehmigung des Datenverantwortlichen einen Unterauftragsverarbeiter mit einer "anderen" als der vereinbarten Verarbeitung zu beauftragen oder einen anderen Unterauftragsverarbeiter mit der beschriebenen Verarbeitung zu beauftragen.

B.2. Vorankündigung für die Zulassung von Unterauftragsverarbeitern

Der Datenverarbeiter informiert den Datenverantwortlichen mindestens 30 Tage vor einer Änderung der Liste der Unterauftragsverarbeiter und gibt dem Datenverantwortlichen die Möglichkeit, Einspruch gegen die Änderung der Liste der Unterauftragsverarbeiter einzulegen. Hat der Datenverantwortliche dem Wechsel des Unterauftragsverarbeiters oder der Beauftragung eines neuen Unterauftragsverarbeiters nicht fristgerecht widersprochen, gilt der Unterauftragsverarbeiter als akzeptiert.

Sollte die Änderung der Liste der Unterauftragsverarbeiter eine Hinzufügung eines Unterauftragsverarbeiters in einem Drittland beinhalten, muss Datenverantwortliche wie in Anhang C, Abschnitt C.6 vereinbart informiert werden.

Anhang C) Anweisung über die Verwendung personenbezogener Daten

C.1. Gegenstand derVerarbeitung/Anweisung zur Verarbeitung

Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen erfolgt durch den Datenverarbeiter in folgender Weise:

Der Datenverarbeiter stellt dem Datenverantwortlichen SameSystem gemäß dem Lizenzvertrag und den allgemeinen Lizenzbedingungen zur Verfügung und speichert zur Erfüllung des Lizenzvertrags personenbezogene Daten im Namen des Datenverantwortlichen, über die Mitarbeiter des Datenverantwortlichen und auf den Servern des Datenverarbeiters und den entsprechenden Servern der Unterauftragsverarbeiter, wie in Anhang B, B1 aufgeführt, beschrieben und vom Datenverantwortlichen genehmigt.

Der Datenverarbeiter ist angewiesen, die personenbezogenen Daten nur zu diesem Zweck zu verarbeiten und ist nicht berechtigt, die personenbezogenen Daten des Datenverantwortlichen für andere Zwecke zu verarbeiten oder zu nutzen.

C.2. Sicherheit der Verarbeitung

In diesem Abschnitt werden die Mindestsicherheitsanforderungen an das interne Sicherheitsniveau und die Kontrollen des Datenverarbeiters dargelegt.

C.2.1.1 Organisation der Informationssicherheit (A.5 Sicherheitsrichtlinie & A.6 Rollen und Verantwortung)

Der Datenverarbeiter muss über eine dokumentierte Sicherheitsrichtlinie verfügen, welche die Informationssicherheit für das gesamte Personal des Datenverarbeiters behandelt. Das Sicherheitskonzept muss mindestens einmal jährlich überprüft und aktualisiert werden. Es muss eine Richtlinie für die Verarbeitung personenbezogener Daten geben - sie kann in die Informationssicherheitsrichtlinie aufgenommen werden. Ein Verzeichnis der Strategien und Verfahren muss jederzeit verfügbar sein und in einer vom Datenverarbeiter festgelegten Häufigkeit gepflegt werden, welche die in den Klauseln vereinbarten Verpflichtungen widerspiegelt.

Eine Informationssicherheitsfunktion muss für die Sicherheitsinitiativen innerhalb der Organisation des Datenverarbeiters verantwortlich sein. Eine namentlich benannte Person muss für die dem Datenverantwortlichen erbrachten Informationssicherheitsdienste verantwortlich sein.

Der Datenverarbeiter muss über einschlägige aktualisierte Risikobewertungen zur Informationssicherheit verfügen, die dem Datenverantwortlichen auf Anfrage zur Verfügung gestellt werden müssen, bevor Dienstleistungen erbracht oder geändert werden.

Der Datenverarbeiter muss eine Risikobewertung des Zugangs anderer externer Parteien zu Daten, Systemen und Netzen vornehmen.

Die Rollen und Zuständigkeiten im Zusammenhang mit der Informationssicherheitsrichtlinie, einschließlich der Verarbeitung personenbezogener Daten, müssen klar definiert und beschrieben werden.

C.2.1.2 Sicherheitsbewusstsein (A.7 Sicherheit der Humanressourcen)

Der Datenverarbeiter muss ein Programm zur Sensibilisierung für Informationssicherheit und Datenschutz einführen, um alle Mitarbeiter zu schulen, die Zugang zu den Daten des Datenverantwortlichen haben oder mit ihnen umgehen können.

C.2.1.3 Asset-Verwaltung und Geräte (A.8 Asset-Verwaltung)

Die Organisation muss über ein Register der IT-Ressourcen verfügen, die für die Verarbeitung personenbezogener Daten im Auftrag des Datenverantwortlichen verwendet werden. Diese Liste muss von einer spezifischen Person geführt werden, die sie auch regelmäßig, mindestens aber jährlich, überprüft und aktualisiert.

Alle Geräte, die für die Handhabung und/oder Verarbeitung der Daten des Datenverantwortlichen relevant sind, einschließlich USB-Sticks und anderer mobiler Geräte, müssen geschützt werden, einschließlich Festplattenverschlüsselung, starker Passwörter zum Schutz vor unbefugtem Zugriff auf personenbezogene Daten und Zugriffsbeschränkung auf Mitarbeiter mit spezifischen arbeitsbezogenen Zwecken.Passwörter müssen in gehashter Form gespeichert

werden.Der Login muss nach fünf fehlgeschlagenen Login-Versuchen automatisch gesperrt werden, um einen unbefugten Zugriff auf personenbezogene Daten zu verhindern.

Wenn personenbezogene Daten auf den persönlichen Geräten der Mitarbeiter des Datenverarbeiters (BYOD) verarbeitet werden können, müssen die Geräte angemessen gesichert sein, einschließlich Verschlüsselung, erzwungener angemessener Passwörter und Beschränkung des Zugriffs auf Mitarbeiter mit spezifischen arbeitsbezogenen Zwecken, z. B. durch Sandboxing-Technologien. BYOD-Richtlinien, -Leitlinien und -Datenschutzrichtlinien müssen dem Datenverantwortlichen auf Anfrage zur Verfügung gestellt werden - dazu gehört auch die Einführung eines Mobile Device Management (MDM)-Tools zur Durchsetzung der oben genannten Bestimmungen.

Der Datenverarbeiter muss die Kontrolle über alle für die Erbringung von Diensten für den Datenverantwortlichen genutzten Assets sicherstellen, damit gewährleistet ist, dass alle Daten des Datenverantwortlichen vor der Stilllegung der Hardware oder der Wiederverwendung für andere Zwecke mit spezieller Software sicher überschrieben werden.

Verwendete externe Datenträger, einschließlich USB-Sticks, Tablets, Smartphones usw., müssen verschlüsselt und sicher gelöscht oder vernichtet werden, wenn sie außer Betrieb genommen werden, um einen unbefugten Zugriff auf personenbezogene Daten zu verhindern.

Festplattenund Wechseldatenträger müssen während der Reparatur, der Wartung und des Transports aufbewahrt und vor unbefugtem Zugriff geschützt werden, und sie müssen gemäß allen Sicherheitsanforderungen behandelt werden.

C.2.1.4 Zugangsverwaltung (A.9 Zugangskontrolle)
Der Datenverarbeiter muss klar definierte Rollen und Verantwortlichkeiten für die Mitarbeiter haben. Vor der Einstellung muss ein entsprechendes Screening durchgeführt werden [das eine Bewertung der folgenden Punkte beinhalten kann: Hintergrundüberprüfung, Strafregister, früherer Arbeitgeber usw.], wobei die Beschäftigungsbedingungen angemessen anzuwenden sind.

Der Datenverarbeiter muss Verfahren für die Benutzerverwaltung einführen, in denen die Benutzerrollen und ihre Berechtigungen sowie die Art und Weise der Gewährung, Änderung und Beendigung des Zugriffs festgelegt sind, die eine angemessene Aufgabentrennung vorsehen und in denen die Anforderungen und Mechanismen für die Protokollierung/Überwachung definiert sind.

Der privilegierte Zugang zu Daten, Anwendungen und Infrastruktur muss auf Personen mit einem spezifischen, dokumentierten Geschäftszweck beschränkt sein. Die Zugriffsrechte und die zulässige Verwendung personenbezogener Daten müssen für die jeweiligen Aufgabenbereiche schriftlich festgelegt werden.

Der Datenverarbeiter muss eine dokumentierte, effiziente und regelmäßige Kontrolle der zugewiesenen Rechte für alle Arten von Benutzerkonten in allen Systemen, welche die Dienste des Datenverantwortlichen unterstützen, sicherstellen. Die Kontrollüberprüfung muss für Endbenutzerkonten mindestens einmal alle zwölf Monate und für privilegierte Konten mindestens einmal alle sechs Monate aktualisiert werden. Bei austretenden oder gekündigten Benutzern müssen die Anmeldedaten unmittelbar nach dem letzten Arbeitstag deaktiviert werden.

Der Datenverarbeiter muss den Datenverantwortlichen bei der Überprüfung seiner eigenen Buchführung unterstützen. Auf Anfrage des Datenverantwortlichen muss der Datenverarbeiter eine Übersicht über die Zugriffsrechte der einzelnen Mitarbeiter auf die Daten und Systeme des Datenverantwortlichen vorlegen.

Allen Mitarbeitern müssen eindeutige Benutzer-IDs zugewiesen werden, und die Neuausstellung von deaktivierten oder abgelaufenen Benutzer-IDs ist verboten.

Die Zugriffsrechte müssen nach dem "Least Privilege"-Prinzip vergeben werden.

Für den privilegierten Zugang zu Daten, Anwendungen und Infrastruktur muss eine Zwei-Faktor-Authentifizierung vorgeschrieben sein.

Der Fernzugriff auf Daten, Anwendungen und Infrastruktur muss eine Zwei-Faktor-Authentifizierung erfordern.

C.2.1.5 Physische Sicherheit (A.11 Physische und Umgebungssicherheit)
Serverräume, Rechenzentren und Büroräume, von denen aus potenziell auf die Daten des Datenverantwortlichen zugegriffen werden kann, müssen vor unbefugtem Zugriff geschützt werden.

Für alle diese Orte muss eine physische Zugangskontrolle eingerichtet werden. Unbefugter Zugang muss durch eine 24x7-Überwachung und Zugangsbeschränkung mit einem elektronischen Zugangsprotokoll verhindert werden. Alle Mitarbeiter und Besucher, die Zugang zu den Räumlichkeiten haben, sollten sich durch geeignete Mittel, z. B. Ausweise, eindeutig identifizieren lassen.

Die Einrichtungen müssen mit entsprechenden technischen Anlagen ausgestattet sein, um die Verfügbarkeit der Dienste zu gewährleisten.

C.2.1.6 Sicherheit vor Ort (A.11 Physische und umgebungsbezogene Sicherheit)
Physische Dokumente müssen sicher gehandhabt und geschützt werden, vom Druck über die sichere Aufbewahrung bis hin zur physischen Vernichtung, z. B. durch den Einsatz von "Follow-Me-Printing" und Druckern, die sich an einem sicheren Ort mit beschränktem Zugang befinden. Aktenschränke müssen an einem gesicherten Ort mit beschränktem Zugang oder in einem gesicherten Lager untergebracht werden. Die Schränke müssen entsprechend der Klassifizierung des darin gelagerten Materials gesichert werden.

Es muss eine physische Zugangskontrolle vorhanden sein, um alle Arten von personenbezogenen Daten auf allen Medien an jedem Standort zu schützen, von Büros und Serverräumen bis hin zu Druckern und Faxgeräten, die Ausdrucke mit personenbezogenen Daten des Datenverantwortlichen erstellen könnten.

Dazu gehört der Schutz vor dem Risiko, dass Unbefugte auf Computerbildschirme schauen, dass Personen Dokumente lesen, die auf den Schreibtischen liegen, dass Reinigungspersonal außerhalb der Geschäftszeiten Zugang hat, dass sensible persönliche Daten in Schränken eingeschlossen sind usw. Um dies zu verhindern, sollte eine "Clean-Desk-Policy" eingeführt werden.

C.2.1.7 Aktualisierung, Patching und Änderungskontrolle (A.12 Betrieb)
Der Datenverarbeiter muss sicherstellen, dass System- und Software-Patches gemäß den Empfehlungen des Anbieters auf allen Systemen und Infrastrukturen, die Dienste für den Datenverantwortlichen erbringen können, installiert werden, einschließlich interner Workstations, Anwendungen und Server.

Der Datenverarbeiter muss die Sicherheitsupdates einspielen. Kritische und wichtige Sicherheits-Patches müssen überprüft und so schnell wie möglich installiert werden.

C.2.1.8 Lieferantenbeziehungen (A.15 Beziehungen zu Unterauftragsverarbeitern)

Falls der Datenverarbeiter einen Unterauftragsverarbeiter einsetzt oder einzusetzen gedenkt:

Bevor die Verarbeitung personenbezogener Daten durch einen Unterauftragsverarbeiter erfolgt, sollten formelle Leitlinien und Verfahren einschließlich einschlägiger vertraglicher Maßnahmen festgelegt werden, welche die vorliegenden Kriterien abdecken. Auf Verlangen des Datenverantwortlichen werden dem Datenverantwortlichen innerhalb eines angemessenen Zeitrahmens und ohne unangemessene Verzögerung die Unterlagen zur Verfügung gestellt, aus denen hervorgeht, dass der Unterauftragsverarbeiter diese Klauseln und/oder die DSGVO und/oder die einschlägigen Rechtsvorschriften der Mitgliedstaaten einhält. Diese Leitlinien, Verfahren und vertraglichen Maßnahmen müssen mindestens das gleiche Niveau des Schutzes und der Sicherheit personenbezogener Daten gewährleisten, wie es in diesen Klauseln vorgeschrieben ist.

C.2.1.9 Schutz vor Malware (A.12 Betriebssicherheit)
Auf allen Systemen und Geräten des Datenverarbeiters, die bei der Verarbeitung personenbezogener Daten im Auftrag des Datenverantwortlichen eingesetzt werden oder mit den vom Datenverarbeiter verwalteten Systemen oder Geräten verbunden sind, muss ein aktueller Schutz vor Schadsoftware installiert und gewartet werden.

C.2.1.10 Backups (A.12 Betriebssicherheit)
Der Datenverarbeiter muss über eine dokumentierte Backup-Richtlinie verfügen und ein Backup der Systeme und Daten des Datenverantwortlichen durchführen. Die Anforderungen an

die Aufbewahrung und Löschung von Daten müssen definiert und in Übereinstimmung mit den Richtlinien und Verfahren gehandhabt werden.

Der Datenverarbeiter muss Verfahren einführen, um Backups zu verifizieren, indem er die gesicherten Daten, Software und Systeme mindestens alle 6 Monate erfolgreich wiederherstellt.Die Dokumentation muss auf Anfrage verfügbar sein und in die KPI/Berichterstattung aufgenommen werden.

Backups müssen vor unberechtigtem Zugriff geschützt werden.

Die Backups müssen verschlüsselt und sicher aufbewahrt werden.

C.2.1.11 Protokollierung und Überwachung (A.12 Betriebssicherheit)
Jeder Zugriff auf personenbezogene Daten muss protokolliert werden. Das Zugriffsprotokoll muss das Datum und die Uhrzeit des Zugriffs, die UserID und die Art des Zugriffs (Lesen, Bearbeiten, Löschen, bei sensible Daten auch Anzeigen und Durchsuchen von Daten usw.) enthalten.

Die Sicherheitsprotokollierung muss auf allen Netzwerkgeräten, Servern und allen Anwendungen, einschließlich Datenbanken und IT-Systemadministratoren, aktiviert werden - die Protokolldateien müssen mit einem Zeitstempel versehen und angemessen gegen Manipulationen und unbefugten Zugriff geschützt werden. Die Uhren sollten mit einer einzigen Zeitquelle synchronisiert werden. Die Protokolle müssen überwacht werden - z. B. durch die Einrichtung von Regeln für Alarme, wenn die Protokolle Anomalien zeigen, auf die der Datenverarbeiter reagieren sollte.

Ein zentralisiertes System zur Sammlung und Überprüfung von Sicherheitsprotokollen muss als solches vorhanden sein.

Die Protokolle über den Zugriff auf personenbezogene Daten und die Verwendung personenbezogener Daten müssen überwacht werden und zur Überprüfung zur Verfügung stehen, um einen unbefugten Zugriff auf personenbezogene Daten festzustellen. Es muss dokumentiert werden, wann und wie oft die Protokolldateien überprüft werden und wer die Kontrolle durchgeführt hat. Die Unterlagen müssen auf Anfrage erhältlich sein.

Fehlgeschlagene Anmeldeversuche müssen protokolliert und 6 Monate lang aufbewahrt werden, um einen unbefugten Zugriff auf personenbezogene Daten zu erkennen.

C.2.1.12 Netzwerksicherheit (A.13 Kommunikationssicherheit)
Der Datenverarbeiter muss die Netzwerksicherheit mit handelsüblichen Geräten und Industriestandardtechniken aufrechterhalten, einschließlich Firewalls und Systemen zur Erkennung von Eindringungsversuchen.

Die Infrastruktur muss segmentiert werden, um zumindest die Produktionssysteme von den Test- und Entwicklungsumgebungen zu trennen.

Alle vom Datenverarbeiter übermittelten personenbezogenen Daten müssen während der Übertragung und im Ruhezustand verschlüsselt werden.

C.2.1.13 Management von Sicherheitsvorfällen (A.16 Management von Vorfällen)
Der Datenverarbeiter muss Verfahren zur schnellen und wirksamen Erkennung, Analyse und Behandlung von Sicherheitsvorfällen einführen.

Alle Sicherheitsvorfälle und -verletzungen im Zusammenhang mit Diensten, die für den Datenverantwortlichen erbracht werden, müssen dem Datenverantwortlichen ohne unnötige Verzögerung gemeldet werden.

Der Datenverarbeiter muss die in der DSGVO festgelegten Meldepflichten erfüllen und dem Datenverantwortlichen innerhalb von 24 Stunden die erforderlichen Informationen übermitteln.

C.2.1.14 Disaster-Recovery und Business-Continuity (A. 17 Aspekte der Informationssicherheit im Rahmen des Business Continuity Management)
Der Datenverarbeiter muss einen dokumentierten und getesteten Notfallwiederherstellungsplan und eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs für die Systeme des Datenverantwortlichen gemäß einem vereinbarten Serviceniveau umsetzen.

Disaster-Recovery-Pläne und Business-Continuity-Strategien müssen regelmäßig, mindestens aber jährlich, getestet und aktualisiert werden, um sicherzustellen, dass sie aktuell und wirksam sind. Die Unterlagen müssen auf Anfrage erhältlich sein.

C.2.1.15 Datenverarbeitung (C.7.3.8)
Der Datenverarbeiter muss in der Lage sein, dem Datenverantwortlichen auf Anfrage eine Kopie aller von ihm verarbeiteten Informationen über eine bestimmte betroffene Person in strukturierter, allgemein verwendeter und maschinenlesbarer Form zur Verfügung zu stellen

C.2.2 Lösungsspezifische Sicherheitsanforderungen

C.2.2.1 Cloud-Dienste
Der Datenverarbeiter führt eine Risikoanalyse der relevanten Cloud-basierten Unterdrücker durch. Die Unterauftragsverarbeitungsverträge des Datenverarbeiters mit etwaigen Cloud-Anbietern, die Teil der Lösung sind, müssen dem Datenverantwortlichen auf Anfrage vorgelegt werden.

C.2.2.2 Sicherheit im Lebenszyklus von Anwendungen (A.14 Erwerb, Entwicklung und Wartung von Systemen)
Während des Lebenszyklus der Entwicklung sollten bewährte Praktiken, der Stand der Technik und anerkannte sichere Entwicklungspraktiken, -rahmen oder -standards befolgt werden, was bedeutet, dass der Datenverarbeiter in allen Phasen des Lebenszyklus der Datenverarbeitung und des Systems die Grundsätze des "Data Protection by Design- and by Default" umsetzen muss. Dazu gehört, dass nur relevante, verhältnismäßige und notwendige Informationen, einschließlich der Verwendung, Offenlegung, Aufbewahrung, Übermittlung und Beseitigung von Daten über Einzelpersonen für die Anwendung, welche die Daten verarbeitet, erfasst werden.

Personenbezogene Daten dürfen nicht in der Entwicklungs- oder Testumgebung verwendet werden, ohne dass sie vor der Verwendung anonymisiert, pseudonymisiert, verschlüsselt oder maskiert werden.

Die Systementwicklung muss in speziellen Entwicklungsumgebungen stattfinden, die von den Produktions- und Testsystemen isoliert sind und vor unbefugtem Zugriff geschützt werden müssen.

Der Quellcode muss vor unbefugtem Zugriff und Verwendung geschützt werden.

Der Datenverarbeiter muss alle Codes und Anwendungen, die für den Datenverantwortlichen entwickelt werden, vor der Freigabe einer Sicherheitsüberprüfung, Schwachstellenprüfung und Penetrationstests unterziehen. Regelmäßige PEN-Tests sollten für Web-Anwendungen durchgeführt und dokumentiert werden.

C.3. Unterstützung für den Datenverantwortlichen
Der Datenverarbeiter unterstützt den Datenverantwortlichen nach Maßgabe der Ziffern 9.1. und 9.2., soweit dies möglich ist, - im Rahmen und im Umfang der nachstehend genannten Unterstützung - durch die Umsetzung der folgenden technischen und organisatorischen Maßnahmen:

Der Datenverarbeiter ist verpflichtet, den Datenverantwortlichen bei der Erfüllung seiner Verpflichtungen aus diesem Vertrag unverzüglich zu unterstützen.

C.4. Aufbewahrungsdauer/Löschverfahren
Die Befugnis des Datenverarbeiters, personenbezogene Daten im Auftrag des Datenverantwortlichen zu verarbeiten, erlischt, wenn die Klauseln oder der Lizenzvertrag beendet werden.

Bei Beendigung der Klauseln geben der Datenverarbeiter und seine Unterauftragsverarbeiter alle personenbezogenen Daten, die der Datenverarbeiter im Rahmen der Klauseln verarbeitet

hat, gemäß Klausel 14 zurück und/oder löschen sie. Der Datenverantwortliche kann eine Dokumentation verlangen.

Der Datenverarbeiter darf jedoch die Verarbeitung personenbezogener Daten bis zu einem Monat nach Beendigung der Klauseln fortsetzen, wenn der Umfang der Daten einen größeren Arbeitsaufwand für den Datenverarbeiter erfordert. Der Datenverarbeiter ist im gleichen Zeitraum berechtigt, die personenbezogenen Daten in das normale Datensicherungsverfahren einfließen zu lassen. Die Verarbeitung personenbezogener Daten durch die Datenverarbeiter in diesem Zeitraum erfolgt nach denselben Anweisungen wie in den Klauseln beschrieben.

C.5. Verarbeitungsort

Die Standorte des Datenverarbeiters und seiner Unterauftragsverarbeiter sind in Anhang B, B.1 aufgeführt.

Die Verarbeitung personenbezogener Daten gemäß den Klauseln kann nicht an anderen als den in Anhang B, B.1 aufgeführten Orten erfolgen. Andere/neue Verarbeitungsorte bedürfen der vorherigen Meldung durch den Datenverarbeiter gemäß Anhang B, B2 in den Klauseln, die besagen, dass der Einsatz eventueller neuer Unterauftragsverarbeiter (und damit eventuell neuer Verarbeitungsorte) dem Datenverantwortlichen mindestens 60 Tage vor dem geplanten Einsatz gemeldet werden sollte.

C.6. Anweisung zur Übermittlung personenbezogener Daten an Drittländer

C.6.1 Der Datenverarbeiter kann Daten an einen Unterauftragsverarbeiter übermitteln, der gemäß Abschnitt 7.3 dieser Vereinbarung zugelassen ist.

C.6.2 Der Datenverarbeiter muss eine Rechtsgrundlage für die Übermittlung gemäß Kapitel V der Datenschutz-Grundverordnung schaffen, ohne dazu der Unterschrift des Datenverantwortlichen zu bedürfen. In diesen Fällen ist der Datenverarbeiter verpflichtet, die Rechtmäßigkeit der Übermittlungsgrundlage sicherzustellen.

C.6.3 Im Falle der Übermittlung von Daten in ein Drittland muss der Datenverantwortliche mindestens 30 Tage vor der Übermittlung informiert werden. Erhebt der Datenverantwortliche innerhalb dieser Frist keine Einwände gegen die Übermittlung, wird die Übermittlung gemäß Klausel 7.3 dieser Vereinbarung genehmigt.

Wenn der Datenverantwortliche keine dokumentierten Anweisungen für die Übermittlung personenbezogener Daten in ein Drittland gemäß diesen Klauseln erteilt, ist der Datenverarbeiter im Rahmen dieser Klauseln nicht berechtigt, eine solche Übermittlung vorzunehmen.

C.7. Verfahren für die vom Datenverantwortlichen durchgeführten Audits, einschließlich Inspektionen, der Verarbeitung personenbezogener Daten durch den Datenverarbeiter

Der Datenverarbeiter muss einmal pro Jahr auf eigene Kosten einen Audit- oder Zertifizierungsbericht von einem unabhängigen Dritten über seine Einhaltung der DSGVO, der geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten und der Klauseln einholen.

Die Parteien sind übereingekommen, dass die folgende Art von Audit und Zertifizierung in Übereinstimmung mit den Klauseln verwendet werden kann:

ISAE3000

Der genehmigte Bericht oder die genehmigte Bescheinigung ist dem für die Verarbeitung Verantwortlichen auf Verlangen unverzüglich vorzulegen, um die Einhaltung der in diesen Klauseln genannten Kriterien nachzuweisen. Der genehmigte Bericht bzw. die genehmigte Be-

scheinigung ist auch unter www.samesystem.com abrufbar. Der für die Verarbeitung Verantwortliche kann den Umfang und/oder die Methodik des Berichts anfechten und in diesem Fall ein neues Audit/eine neue Inspektion mit einem geänderten Umfang und/oder einer anderen Methodik verlangen. Der Datenverarbeiter ist berechtigt, einen angemessenen Stundensatz für die in Anhang D dieser Klauseln geregelte Dienstleistung in Rechnung zu stellen, wenn der für die Verarbeitung Verantwortliche andere Audits und/oder Zertifizierungen als die oben genannten verlangt.

Auf der Grundlage der Ergebnisse eines solchen Audits/einer solchen Inspektion kann der Datenverantwortliche verlangen, dass weitere Maßnahmen ergriffen werden, um die Einhaltung der DSGVO, der geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten und der Klauseln zu gewährleisten.

Der Datenverantwortliche oder der Vertreter des Datenverantwortlichen hat darüber hinaus das Recht, die Orte zu inspizieren, an denen die Verarbeitung personenbezogener Daten durch den Datenverarbeiter erfolgt, einschließlich der physischen Einrichtungen sowie der Systeme, die für die Verarbeitung im Auftrag des Datenverantwortlichen verwendet werden und damit im Zusammenhang stehen. Eine solche Kontrolle wird durchgeführt, wenn der Datenverantwortliche sie für erforderlich hält und wenn sie einen konkreten und relevanten Zweck hat.

C.8. Verfahren für Audits, einschließlich Inspektionen, der Verarbeitung personenbezogener Daten durch Unterauftragsverarbeiter

Das Audit oder die Zertifizierung, wie in diesem Anhang Abschnitt C.7 vereinbart, muss die Unterauftragsverarbeiter, die bei der erbrachten Dienstleistung eingesetzt werden, in den Umfang des Audits oder der Zertifizierung einbeziehen.

Wenn die Unterauftragsverarbeiter nicht Teil des Umfangs des vereinbarten Audits oder der Zertifizierung nach C.7 sind,
muss der Datenverarbeiter einmal jährlich auf eigene Kosten ein Audit oder eine Bescheinigung eines unabhängigen Dritten über die Einhaltung der DSGVO, der geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten und der Klauseln durch den Unterauftragsverarbeiter einholen oder eine entsprechende Inspektion des Unterauftragsverarbeiters gemäß den oben genannten oder ähnlichen Standards, wie in Abschnitt C.7 erwähnt, durchführen.

Der genehmigte Bericht oder die genehmigte Bescheinigung ist dem Datenverantwortlichen auf Verlangen unverzüglich vorzulegen, um die Einhaltung der in diesen Klauseln genannten Kriterien nachzuweisen. Der Datenverantwortliche kann den Umfang und/oder die Methodik des Berichts anfechten und in diesem Fall ein neues Audit/eine neue Inspektion mit geändertem Umfang und/oder anderer Methodik verlangen. Der Datenverarbeiter ist berechtigt, einen angemessenen Stundensatz für die Dienstleistung in Rechnung zu stellen, wenn der Datenverantwortliche andere als die oben genannten Audits und/oder Zertifizierungen verlangt.

Auf der Grundlage der Ergebnisse eines solchen Audits/einer solchen Inspektion kann der Datenverantwortliche verlangen, dass weitere Maßnahmen ergriffen werden, um die Einhaltung der DSGVO, der geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten und der Klauseln zu gewährleisten.

Der Datenverarbeiter oder der Vertreter des Datenverarbeiters hat darüber hinaus Zugang zu den Orten, an denen die Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter erfolgt, einschließlich der physischen Einrichtungen sowie der für die Verarbeitung verwendeten und damit im Zusammenhang stehenden Systeme, und kann diese auch physisch inspizieren. Eine solche Kontrolle wird durchgeführt, wenn der Datenverarbeiter (oder der Datenverantwortliche) sie für erforderlich hält und wenn sie einen konkreten und relevanten Zweck hat.

Die Unterlagen für solche Kontrollen sind dem Datenverantwortlichen unverzüglich zur Kenntnisnahme vorzulegen. Der Datenverantwortliche kann den Umfang und/oder die Methodik des Berichts anfechten und in solchen Fällen eine neue Inspektion mit geändertem Umfang und/oder anderer Methodik verlangen, wenn dies einen konkreten und relevanten Zweck hat.

Der Datenverantwortliche kann - falls erforderlich - eine physische Kontrolle des Unterauftragsverarbeiters veranlassen und daran teilnehmen. Dies kann der Fall sein, wenn der Datenverantwortliche der Ansicht ist, dass die Kontrolle des Unterauftragsverarbeiters durch den

Datenverarbeiter dem Datenverantwortlichen keine ausreichenden Unterlagen zur Verfügung gestellt hat, anhand derer er feststellen kann, dass die Verarbeitung durch den Unterauftragsverarbeiter im Einklang mit den Klauseln durchgeführt wird.

Die Teilnahme des Datenverantwortlichen an einer Inspektion des Unterauftragsverarbeiters ändert nichts an der Tatsache, dass der Datenverarbeiter weiterhin die volle Verantwortung dafür trägt, dass der Unterauftragsverarbeiter die Datenschutz-Grundverordnung, die geltenden Datenschutzbestimmungen der EU oder der Mitgliedstaaten und die Klauseln einhält.

Die Kosten des Datenverarbeiters und des Unterauftragsverarbeiters im Zusammenhang mit der physischen Überwachung/Inspektion in den Einrichtungen des Unterauftragsverarbeiters gehen nicht zu Lasten des Datenverantwortlichen - unabhängig davon, ob der Datenverantwortliche eine solche Inspektion veranlasst und daran teilgenommen hat, sofern sie einen konkreten und relevanten Zweck hat.

Anhang D) Die Vereinbarung der Parteien zu anderen Themen

In Bezug auf 9.2 und C.7

Soweit der für die Datenverarbeitung Verantwortliche die Unterstützung des Datenverarbeiters bei den in Abschnitt 9.2 (c) und (d) beschriebenen Dienstleistungen in Anspruch nimmt und für den Fall, dass der für die Datenverarbeitung Verantwortliche andere als die oben in Anhang C, Abschnitt C.7 genannten Prüfungen oder/und Zertifizierungen verlangt, ist der für die Datenverarbeitung Verantwortliche verpflichtet, den Datenverarbeiter für die hierfür aufgewendete Zeit zu den vom Datenverarbeiter zu jeder Zeit verwendeten Stundensätzen zu vergüten.

Änderungen der Vereinbarung über die Datenverarbeitung

Zwischen den Parteien gilt immer die aktuellste Version der Datenverarbeitungsvereinbarung.

Der Datenverarbeiter behält sich das Recht vor, laufend Änderungen und Klarstellungen an der Vereinbarung vorzunehmen. Diese Änderungen ergeben sich in der Regel aus neuen Empfehlungen, z. B. der Datenschutzbehörde oder der EU-Kommission, sowie aus Änderungen der Praxis und der Gesetzgebung in diesem Bereich.

Der für die Verarbeitung Verantwortliche wird daher gebeten, sich für den Erhalt von Benachrichtigungen bei Änderungen des Abkommens anzumelden.

Der für die Verarbeitung Verantwortliche hat nach Erhalt einer Benachrichtigung über eine Änderung 14 Arbeitstage Zeit, um Einspruch zu erheben, wenn die Änderung vernünftigerweise nicht akzeptiert werden kann.

Diese Bestimmung gilt nicht für Änderungen bei der Nutzung von Unterauftragsverarbeitern, die in Abschnitt 7 des Abkommens geregelt sind.