DATENVERARBEITUNGSVEREINBARUNG

VERSION 4.1 NOVEMBER 2025

CompuSoft A/S

Sunekaer 9

5471 Soendersoe

Dänemark

VAT DK21774774

Standard-Vertragsbestimmungen

gemäß Artikel 28 Abs. 3 der Verordnung (EU) 2016/679 (Datenschutzverordnung) für die Verarbeitung personenbezogener Daten durch den Datenverarbeiter

zwischen

«COMPANY»
USt-IdNr «COMPANYCVR»
«COMPANYADRESS»
«COMPANYCITY»

nachstehend „der Datenverantwortliche“ genannt,

und

CompuSoft A/S
VAT DK21774774
Sunekaer 9
DK-5471 Soendersoe

nachstehend „der Datenverarbeiter“ genannt,

die jeweils eine „Partei“ sind und zusammen die „Parteien“ bilden

HABEN die folgenden Standardvertragsbestimmungen (die Bestimmungen) vereinbart, um die Datenschutzverordnung einzuhalten und den Schutz der Privatsphäre sowie der Grundrechte und Grundfreiheiten natürlicher Personen zu gewährleisten

1. INHALT

2. PRÄAMBEL

1. Diese Bestimmungen legen die Rechte und Pflichten des Datenverarbeiters fest, wenn er personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet.

2. Diese Bestimmungen sollen gewährleisten, dass Artikel 28 Abs. 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) von den Parteien eingehalten wird.

3. Im Zusammenhang mit der Erbringung des Buchungs- und Zahlungssystems des Datenverarbeiters, wie näher in den BEDINGUNGEN für das Hosting von CompuSoft ("**Hauptvertrag**“) angegeben, verarbeitet der Datenverarbeiter personenbezogene Daten im Auftrag des Datenverantwortlichen gemäß diesen Bestimmungen.

4. Die Bestimmungen haben Vorrang vor etwaigen entsprechenden Bestimmungen in anderen Vereinbarungen zwischen den Parteien.

5. Es gibt vier Anhänge zu diesen Bestimmungen, die einen integralen Bestandteil der Bestimmungen bilden.

6. Anhang A enthält detaillierte Informationen zur Verarbeitung personenbezogener Daten, einschließlich des Zwecks und der Art der Verarbeitung, der Art der personenbezogenen Daten, der Kategorien betroffener Personen und der Dauer der Verarbeitung.

7. Anhang B enthält die Bedingungen des Datenverantwortlichen für den Einsatz von Unterauftragsverarbeitern durch den Datenverarbeiter und eine Liste von Unterauftragsverarbeitern, deren Inanspruchnahme der Datenverantwortliche genehmigt hat.

8. Anhang C enthält die Weisungen des Datenverantwortlichen bezüglich der Verarbeitung personenbezogener Daten durch den Datenverarbeiter, eine Beschreibung der Sicherheitsmaßnahmen, die der Datenverarbeiter mindestens umsetzen muss, und wie der Datenverarbeiter und etwaige Unterauftragsverarbeiter beaufsichtigt werden.

9. Anhang D enthält Bestimmungen zu anderen Aktivitäten, die nicht unter die vorliegenden Bestimmungen fallen.

10. Die Bestimmungen mit dazugehörigen Anlagen sind von beiden Parteien schriftlich, auch elektronisch, aufzubewahren.

11. Diese Bestimmungen entbinden den Datenverarbeiter nicht von Verpflichtungen, die dem Datenverarbeiter nach der Datenschutzverordnung oder anderen Gesetzen auferlegt werden.

3. RECHTE UND PFLICHTEN DES DATENVERANTWORTLICHEN

1. Der Datenverantwortliche hat sicherzustellen, dass die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutzverordnung (siehe Artikel 24 der Verordnung), den Datenschutzbestimmungen laut sonstigem EU-Recht oder laut nationalem Recht der Mitgliedstaaten[1] sowie gemäß den vorliegenden Bestimmungen erfolgt.

2. Der Datenverantwortliche hat das Recht und die Pflicht, Entscheidungen darüber zu treffen, für welche(n) Zweck(e) und mit welchen Mitteln personenbezogene Daten verarbeitet werden dürfen.

3. Der Datenverantwortliche hat unter anderem sicherzustellen, dass es eine Verarbeitungsgrundlage für die Verarbeitung personenbezogener Daten gibt, mit deren Durchführung der Datenverarbeiter beauftragt ist.

4. DER DATENVERARBEITER HANDELT NACH WEISUNG

1. Der Datenverarbeiter darf personenbezogene Daten nur gemäß den dokumentierten Weisungen des Datenverantwortlichen verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Datenverarbeiter unterliegt, hierzu verpflichtet ist. Diese Weisungen müssen in den Anhängen A und C angegeben werden. Spätere Weisungen können auch während der Verarbeitung personenbezogener Daten durch den Datenverantwortlichen erteilt werden, aber die Weisungen müssen immer zusammen mit den vorliegenden Bestimmungen schriftlich dokumentiert und aufbewahrt werden, auch in elektronischer Form.

2. Der Datenverarbeiter unterrichtet den Datenverantwortlichen unverzüglich, wenn eine Weisung nach Ansicht der betreffenden Person gegen diese Verordnung oder gegen Datenschutzbestimmungen laut sonstigem EU-Recht oder dem nationalen Recht der Mitgliedstaaten verstößt.

5. VERTRAULICHKEIT

1. Der Datenverarbeiter darf die im Auftrag des Datenverantwortlichen verarbeiteten personenbezogenen Daten nur Personen zugänglich machen, die der Weisungsbefugnis des Datenverarbeiters unterliegen, sich zur Verschwiegenheit verpflichtet haben oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen, und nur im erforderlichen Umfang. Die Liste der Personen, denen der Zugriff gewährt wurde, muss laufend überprüft werden. Basierend auf dieser Überprüfung kann der Zugriff auf personenbezogene Daten gesperrt werden, wenn der

1 Bezugnahmen auf „Mitgliedstaat“ in diesen Bestimmungen sind als Bezugnahmen auf „EWR-Mitgliedstaaten“ zu verstehen.

Zugriff nicht mehr erforderlich ist, und die personenbezogenen Daten dürfen diesen Personen dann nicht mehr zur Verfügung stehen.

2. Auf Verlangen des Datenverantwortlichen muss der Datenverarbeiter nachweisen können, dass die betreffenden Personen, die der Weisungsbefugnis des Datenverarbeiters unterliegen, der oben genannten Geheimhaltungspflicht unterliegen.

6. VERARBEITUNGSSICHERHEIT

1. Artikel 32 der Datenschutzverordnung besagt, dass der Datenverantwortliche und der Datenverarbeiter unter Berücksichtigung des aktuellen technischen Stands, der Implementierungskosten und der Art, des Umfangs, des Kontexts und des Zwecks der betreffenden Verarbeitung sowie der unterschiedlich wahrscheinlichen und schwerwiegenden Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu ergreifen haben, um ein diesen Risiken angemessenes Schutzniveau zu gewährleisten.

   Der Datenverantwortliche muss die Risiken für die Rechte und Freiheiten natürlicher Personen bewerten, die die Verarbeitung mit sich bringt, und Maßnahmen ergreifen, um diesen Risiken zu begegnen. Abhängig von ihrer Relevanz kann dies Folgendes umfassen:

   a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten

   b. die Fähigkeit, fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Robustheit von Verarbeitungssystemen und -diensten sicherzustellen

   c. die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls umgehend wiederherzustellen

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

2. Gemäß Artikel 32 der Verordnung muss der Datenverarbeiter – unabhängig vom Datenverantwortlichen – auch die Risiken für die Rechte natürlicher Personen bewerten, die die Verarbeitung mit sich bringt, und Maßnahmen ergreifen, um diesen Risiken zu begegnen. Für diese Bewertung muss der Datenverantwortliche dem Datenverarbeiter die notwendigen Informationen zur Verfügung stellen, die es ihm ermöglichen, solche Risiken zu erkennen und zu bewerten.

3. Darüber hinaus muss der Datenverarbeiter den Datenverantwortlichen bei der Erfüllung der Verpflichtung des Datenverantwortlichen gemäß Artikel 32 der Verordnung unterstützen, z. B. muss er dem Datenverantwortlichen die erforderlichen Informationen über die technischen und organisatorischen Sicherheitsmaßnahmen zur Verfügung stellen, die der Datenverarbeiter gemäß Artikel 32 der Verordnung bereits umgesetzt hat, sowie alle anderen Informationen, die der Datenverantwortliche benötigt, um seiner Verpflichtung gemäß Artikel 32 der Verordnung nachzukommen.

Wenn die Bewältigung der identifizierten Risiken – nach Einschätzung des Datenverantwortlichen – die Umsetzung zusätzlicher Maßnahmen als diejenigen erfordert, die der Datenverarbeiter bereits umgesetzt hat, muss der Datenverantwortliche die zusätzlich umzusetzenden Maßnahmen in Anhang C angeben.

7. EINSATZ VON UNTERAUFTRAGSVERARBEITERN

1. Der Datenverarbeiter muss im Zusammenhang mit der Beauftragung eines anderen Datenverarbeiters (Unterauftragsverarbeiter) die in der Datenschutzverordnung, Artikel 28, Abs. 2 und 4, genannten Bedingungen erfüllen.

2. Daher darf der Datenverarbeiter zur Erfüllung dieser Bestimmungen ohne vorherige ausdrückliche schriftliche Zustimmung des Datenverantwortlichen keinen Unterauftragsverarbeiter einsetzen.

3. Der Datenverarbeiter darf Unterauftragsverarbeiter nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Datenverantwortlichen einsetzen. Der Datenverarbeiter muss den Antrag auf eine spezifische Zustimmung mindestens zwei Monate vor dem Einsatz des betreffenden Unterauftragsverarbeiters stellen. Die Liste der Unterauftragsverarbeiter, die der Datenverantwortliche bereits genehmigt hat, geht aus Anhang B hervor.

4. Wenn der Datenverarbeiter im Zusammenhang mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Datenverantwortlichen einen Unterauftragsverarbeiter einsetzt, muss der Datenverarbeiter durch einen Vertrag oder ein anderes Rechtsdokument nach EU-Recht oder dem nationalen Recht der Mitgliedstaaten dem Unterauftragsverarbeiter die gleichen Datenschutzpflichten auferlegen, wie sie sich aus diesen Bestimmungen ergeben. Hierbei sind insbesondere die erforderlichen Garantien dafür vorzusehen, dass der Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen so umsetzt, dass die Verarbeitung den Anforderungen dieser Bestimmungen und der Datenschutzverordnung entspricht.

   Der Datenverarbeiter ist daher dafür verantwortlich, dass der Unterauftragsverarbeiter zumindest die Verpflichtungen des Datenverarbeiters gemäß diesen Bestimmungen und der Datenschutzverordnung einhält.

5. Vereinbarung(en) für Unterauftragsverarbeiter und alle nachfolgenden Änderungen daran werden – auf Anfrage des Datenverantwortlichen – in Kopie an den Datenverantwortlichen gesendet, der dadurch die Möglichkeit hat sicherzustellen, dass dem Unterauftragsverarbeiter entsprechende Datenschutzverpflichtungen, die sich aus diesen Bestimmungen ergeben, auferlegt werden. Bestimmungen zu Handelsklauseln, die den datenschutzrechtlichen Inhalt der Unterauftragsverarbeitervereinbarung nicht berühren, sind dem Datenverantwortlichen nicht zu übermitteln.

6. Der Datenverarbeiter muss den Datenverantwortlichen in seiner Vereinbarung mit dem Unterauftragsverarbeiter als begünstigten Dritten im Falle der Insolvenz des Datenverarbeiters einbeziehen, damit der Datenverantwortliche in die Rechte des Datenverarbeiters eintreten und sie

gegenüber Unterauftragsverarbeitern geltend machen. Dies ermöglicht es dem Datenverantwortlichen beispielsweise, den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7. Wenn der Datenverarbeiter seinen Datenschutzverpflichtungen nicht nachkommt, bleibt der Datenverarbeiter gegenüber dem Datenverantwortlichen für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters voll haftbar. Dies berührt nicht die Rechte der betroffenen Personen, die sich aus der Datenschutzverordnung ergeben, einschließlich insbesondere der Artikel 79 und 82 der Verordnung, gegenüber dem Datenverantwortlichen und dem Datenverarbeiter, einschließlich des Unterauftragsverarbeiters.

8. ÜBERMITTLUNG AN DRITTLÄNDER ODER INTERNATIONALE ORGANISATIONEN

1. Jede Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen darf vom Datenverarbeiter nur auf der Grundlage dokumentierter Weisungen des Datenverantwortlichen durchgeführt werden und muss immer in Übereinstimmung mit Kapitel V der Datenschutzverordnung erfolgen.

2. Wenn die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, mit der der Datenverarbeiter nicht im Auftrag des Datenverantwortlichen beauftragt wurde, nach Unionsrecht oder nationalem Recht der Mitgliedstaaten, dem der Datenverarbeiter unterliegt, erforderlich ist, muss der Datenverarbeiter den Datenverantwortlichen vor der Verarbeitung über diese gesetzliche Verpflichtung informieren, es sei denn, das betreffende Gesetz verbietet eine solche Benachrichtigung aus Gründen wichtiger gesellschaftlicher Interessen.

3. Ohne dokumentierte Weisungen des Datenverantwortlichen kann der Datenverarbeiter im Rahmen dieser Verordnung Folgendes nicht tun:

    a. personenbezogener Daten an einen Datenverantwortlichen oder Datenverarbeiter in einem Drittland oder einer internationalen Organisation übermitteln
    b. die Verarbeitung personenbezogener Daten einem Unterauftragsverarbeiter in einem Drittland anvertrauen
    c. die personenbezogenen Daten in einem Drittland verarbeiten

4. Die Weisungen des Datenverantwortlichen bezüglich der Übermittlung personenbezogener Daten in ein Drittland, einschließlich der möglichen Übermittlungsgrundlage laut Kapitel V der Datenschutzverordnung, auf der die Übermittlung beruht, sind in Anhang C.6 anzugeben.

5. Die vorliegenden Bestimmungen sind nicht mit Standardvertragsbestimmungen im Sinne von Artikel 46, Abs. 2, Buchstabe c und d, der Datenschutzverordnung zu verwechseln und die vorliegenden Bestimmungen können keine Grundlage für die Übermittlung personenbezogener Daten im Sinne von Kapitel V der Datenschutzverordnung darstellen.

9. UNTERSTÜTZUNG DES DATENVERANTWORTLICHEN

1. Der Datenverarbeiter unterstützt den Datenverantwortlichen unter Berücksichtigung der Art der Verarbeitung so weit wie möglich durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Verpflichtung des Datenverantwortlichen, auf Anfragen zur Ausübung der Rechte der betroffenen Person, wie in Kapitel III der Datenschutzverordnung dargelegt, zu reagieren.

   Dies bedeutet, dass der Datenverarbeiter den Datenverantwortlichen so weit wie möglich dabei unterstützen muss, die Einhaltung von Folgendem sicherzustellen:

   a. die Informationspflicht bei der Erhebung personenbezogener Daten bei der betroffenen Person
   b. die Informationspflicht, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden
   c. das Recht auf Einsichtnahme
   d. das Recht auf Berichtigung
   e. das Recht auf Löschung („das Recht auf Vergessenwerden“)
   f. das Recht auf Einschränkung der Verarbeitung
   g. die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
   h. das Recht auf Datenübertragbarkeit
   i. das Widerspruchsrecht
   j. das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profilierung, beruht

2. Zusätzlich zu der Verpflichtung des Datenverarbeiters, den Datenverantwortlichen gemäß Bestimmung 6.3 zu unterstützen, unterstützt der Datenverarbeiter den Datenverantwortlichen auch unter Berücksichtigung der Art der Verarbeitung und der dem Datenverarbeiter zur Verfügung stehenden Informationen bei Folgendem:

   a. der Verpflichtung des Datenverantwortlichen, eine Verletzung der Sicherheit personenbezogener Daten der zuständigen Aufsichtsbehörde, der dänischen Datenschutzbehörde, unverzüglich und möglichst spätestens 72 Stunden, nachdem er davon Kenntnis erlangt hat, zu melden, es sei denn, es ist unwahrscheinlich, dass die Verletzung der Sicherheit personenbezogener Daten ein Risiko für die Rechte oder Freiheiten natürlicher Personen birgt

   b. der Verpflichtung des Datenverantwortlichen, die betroffene Person unverzüglich über eine Verletzung der Sicherheit personenbezogener Daten zu informieren, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt

   c. der Verpflichtung des Datenverantwortlichen, vor der Verarbeitung eine Abschätzung der Folgen der beabsichtigten Verarbeitungstätigkeiten zum Schutz personenbezogener Daten durchzuführen (Folgenabschätzung)

d. der Verpflichtung des Datenverantwortlichen, vor der Verarbeitung die zuständige Aufsichtsbehörde, die dänische Datenschutzbehörde, zu konsultieren, wenn eine Datenschutz-Folgenabschätzung zeigt, dass die Verarbeitung zu einem hohen Risiko führen wird, wenn der Datenverantwortliche keine Maßnahmen zur Risikobegrenzung ergriffen hat

3. Die Parteien müssen in Anhang C die erforderlichen technischen und organisatorischen Maßnahmen festlegen, bei denen der Datenverarbeiter den Datenverantwortlichen unterstützen muss, und in welchem Umfang. Dies gilt für die Verpflichtungen aus den Bestimmungen 9.1 und 9.2.

10. BENACHRICHTIGUNG ÜBER EINE VERLETZUNG DER SICHERHEIT PERSONENBEZOGENER DATEN

1. Der Datenverarbeiter benachrichtigt den Datenverantwortlichen unverzüglich, nachdem er Kenntnis davon erlangt hat, dass eine Verletzung der Sicherheit personenbezogener Daten aufgetreten ist.

2. Die Benachrichtigung des Datenverarbeiters an den Datenverantwortlichen muss nach Möglichkeit spätestens 12 Stunden, nachdem dieser von der Verletzung Kenntnis erlangt hat, erfolgen, damit der Datenverantwortliche seiner Verpflichtung nachkommen kann, die Verletzung der Sicherheit personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden; vgl. Artikel 33 der Datenschutzverordnung.

3. Gemäß Bestimmung 9.2.a muss der Datenverarbeiter den Datenverantwortlichen bei der Meldung der Verletzung an die zuständige Aufsichtsbehörde unterstützen. Dies bedeutet, dass der Datenverarbeiter bei der Bereitstellung der folgenden Informationen behilflich sein muss, die gemäß Artikel 33, Abs. 3, aus der Meldung der Verletzung durch den Datenverantwortlichen an die zuständige Aufsichtsbehörde hervorgehen müssen:

   a. die Art der Verletzung der Sicherheit personenbezogener Daten, einschließlich, falls möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Datensätze mit personenbezogenen Daten

   b. die wahrscheinlichen Folgen der Verletzung der Sicherheit personenbezogener Daten

   c. die Maßnahmen, die der Datenverantwortliche ergriffen hat oder zu ergreifen beabsichtigt, um die Verletzung der Sicherheit personenbezogener Daten zu beheben, einschließlich, falls relevant, Maßnahmen zur Begrenzung möglicher nachteiliger Auswirkungen

4. Die Parteien müssen in Anhang D die Informationen angeben, die der Datenverarbeiter im Zusammenhang mit seiner Unterstützung des Datenverantwortlichen bei seiner Verpflichtung zur Meldung von Verletzungen der Sicherheit personenbezogener Daten an die zuständige Aufsichtsbehörde bereitstellen muss.

11. LÖSCHUNG UND RÜCKGABE VON DATEN

1. Bei Beendigung der Dienstleistungen zur Verarbeitung personenbezogener Daten ist der Datenverarbeiter verpflichtet, alle personenbezogenen Daten zurückzugeben und vorhandene Kopien zu löschen, es sei denn, das EU-Recht oder das nationale Recht der Mitgliedstaaten schreibt die Aufbewahrung der personenbezogenen Daten vor.

2. Die folgenden Vorschriften des EU-Rechts oder des nationalen Rechts der Mitgliedstaaten schreiben die Aufbewahrung der personenbezogenen Daten nach Beendigung der Dienstleistungen zur Verarbeitung personenbezogener Daten vor:

   Arkivloven (dänisches Archivgesetz) – Gesetzesdekret Nr. 1201 vom 28.09.2016

   Der Datenverarbeiter verpflichtet sich, die personenbezogenen Daten nur für den/die Zweck(e), während des Zeitraums und unter den Bedingungen zu verarbeiten, die in diesen Vorschriften festgelegt sind.

12. AUDIT, EINSCHLIEßLICH INSPEKTION

1. Der Datenverarbeiter stellt dem Datenverantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung von Artikel 28 der Datenschutzverordnung und dieser Bestimmungen nachzuweisen, und ermöglicht Audits, einschließlich Inspektionen, die vom Datenverantwortlichen oder einem anderen autorisierten Auditor des Datenverantwortlichen durchgeführt werden, und trägt zu diesen bei.

2. Die Verfahren für die Audits des Datenverantwortlichen, einschließlich Inspektionen, beim Datenverarbeiter und den Unterauftragsverarbeitern sind in Anhang C.7 und C.8 aufgeführt.

3. Der Datenverarbeiter ist verpflichtet, Aufsichtsbehörden, die nach geltendem Recht Zugang zu den Einrichtungen des Datenverantwortlichen oder des Datenverarbeiters haben, oder Vertretern, die im Auftrag der Aufsichtsbehörde handeln, gegen ordnungsgemäße Identifizierung Zugang zu den physischen Einrichtungen des Datenverarbeiters zu gewähren.

13. ANDERE VEREINBARUNGEN DER PARTEIEN

1. Die Parteien können andere Bestimmungen bezüglich der Dienstleistungen zur Verarbeitung personenbezogener Daten vereinbaren, z. B. zur Haftung, sofern diese anderen Bestimmungen den vorliegenden Bestimmungen nicht direkt oder indirekt widersprechen oder die sich aus der Datenschutzverordnung ergebenden Grundrechte und Grundfreiheiten der betroffenen Person beeinträchtigen.

14. INKRAFTTRETEN UND BEENDIGUNG

1. Die Bestimmungen treten am Datum der Unterzeichnung durch beide Parteien in Kraft.

2. Beide Parteien können eine Neuverhandlung der Bestimmungen verlangen, wenn Gesetzesänderungen oder Unzulänglichkeiten der Bestimmungen Anlass dazu geben.

3. Die Bestimmungen gelten so lange, wie die Dienstleistungen zur Verarbeitung personenbezogener Daten andauern. Während dieser Zeit können die Bestimmungen nicht gekündigt werden, es sei denn, es werden andere Bestimmungen zur Erbringung der Dienstleistungen zur Verarbeitung personenbezogener Daten zwischen den Parteien vereinbart.

4. Wenn die Bereitstellung der Dienstleistungen zur Verarbeitung personenbezogener Daten eingestellt wird und die personenbezogenen Daten gelöscht oder gemäß Bestimmung 11.1 und Anhang C.4 an den Datenverantwortlichen zurückgegeben werden, können die Bestimmungen von jeder der Parteien durch schriftliche Mitteilung gekündigt werden.

5. Unterzeichnung

Für den Datenverantwortlichen

Name	«PERSONSIGNATURETEXT»
Position	«PERSONPOSITION»
Telefonnummer	«PERSONPHONENUMBER»
E-Mail	«PERSONEMAIL»

Datum und Unterschrift: «KundeUndeskriftDato»

Für den Datenverarbeiter

Name	Kim Wolters
Position	Direktor
Telefonnummer	+45 63186318
E-Mail	KWS@COMPUSOFT.COM

Datum und Unterschrift: «CSSIGNATUREDATE»

15. KONTAKTPERSONEN BEIM DATENVERANTWORTLICHEN UND BEIM DATENVERARBEITER

1. Die Parteien können sich über die untenstehenden Kontaktpersonen kontaktieren.

2. Die Parteien sind verpflichtet, sich gegenseitig laufend über Änderungen von Kontaktpersonen zu informieren.

Name	«PERSONSIGNATURETEXT»
Position	«PERSONPOSITION»
Telefonnummer	«PERSONPHONENUMBER»
E-Mail	«PERSONEMAIL»

Name	Kim Wolters
Position	Direktor
Telefonnummer	+45 63186318
E-Mail	KWS@COMPUSOFT.COM

ANHANG A INFORMATIONEN ZUR VERARBEITUNG

CompuSoft A/S bietet als Datenverarbeiter eine Reihe von IT-Dienste an, die Folgendes umfassen: Hosting, Buchungen und Zahlungen ("**Das System**"). Die Verarbeitung wird unten näher beschrieben.

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

Die Zwecke bestehen darin, den Mitarbeitern des Datenverantwortlichen Zugang zu einem System zu verschaffen, das ihnen dabei helfen kann, die Buchungen und Tickets des Kunden zu verwalten sowie in diesem Zusammenhang Zahlungen einzuziehen und Rechnungen auszustellen, technischen Support, Fehlerbehebung und Wartung des Systems zu leisten sowie vor Betrug, unrechtmäßigen Handlungen und Sicherheitsverstößen zu schützen.

A.2. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen betrifft in erster Linie Folgendes (Art der Verarbeitung)

Erhebung, Registrierung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung personenbezogener Daten gemäß den Weisungen des Datenverantwortlichen.

A.3. Die Verarbeitung umfasst die folgenden Arten von personenbezogenen Daten der betroffenen Personen

Allgemeine personenbezogene Daten (vgl. Artikel 6 der Datenschutzverordnung)

☐Allgemeine personenbezogene Daten:

Kunden und Gäste: Name, Adresse, Postleitzahl, Ort, Nationalität, Telefonnummer, Kreditkartendaten, Korrespondenz, Inhalt der Freitextfelder, gekaufte Produkte, E-Mail-Adresse und in bestimmten Fällen persönliche Identifikationsnummer für staatliche und kommunale Kunden. Darüber hinaus werden gegebenenfalls Aufenthaltsdauer, Anzahl der Personen, Alter und Geschlecht erfasst.

Mitarbeiter: Name, Adresse, Telefonnummer und E-Mail-Adresse.

Sensible personenbezogene Daten über Folgendes (vgl. Artikel 9 der Datenschutzverordnung):

☐Rasse oder ethnische Herkunft

☐Politische Überzeugung

☐Religiöse Überzeugung

☐Philosophische Überzeugung

☐Gewerkschaftszugehörigkeit

☐Genetische Daten

☐Biometrische Daten

☐Gesundheitsinformationen, einschließlich Missbrauch von Medikamenten, Drogen, Alkohol usw.

☐Sexuelle Beziehung oder sexuelle Orientierung einer natürlichen Person

Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (vgl. Artikel 10 der Datenschutzverordnung):

☐Strafrechtliche Verurteilungen

☐Straftaten

Informationen zur CPR-Nummer (persönliche Identifikationsnummer) (vgl. § 11 Datenschutzgesetz)

☐CPR-Nummern (in besonderen Fällen und ausschließlich, wenn der Datenverantwortliche eine Kommune oder staatliche Organisation ist, und nur in dem Umfang, in dem dies für den Datenverantwortlichen zum Zwecke des Zahlungseinzugs erforderlich ist)

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

- Kunden, potenzielle Kunden und Gäste
- Mitarbeiter

A.5. Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen kann nach Inkrafttreten der vorliegenden Bestimmungen beginnen. Die Verarbeitung hat die folgende Dauer

Bis zur Vertragsauflösung.

ANHANG B UNTERAUFTRAGSVERARBEITER

B.1. Zugelassene Unterauftragsverarbeiter

Bei Inkrafttreten der Bestimmungen hat der Datenverantwortliche die Inanspruchnahme der folgenden Unterauftragsverarbeiter genehmigt:

NAME	UST-IDNR	ADRESSE	BESCHREIBUNG DER VERARBEITUNG
Cloudflare Inc.		101 Townsend Street, San Francisco, California, 94107 USA. Der Support-Zugriff kann aus den USA erfolgen. ClaudeFlare Inc. ist nach dem EU-U.S. Data Privacy Framework zertifiziert. Allerdings erfolgt die Speicherung der Informationen direkt nur über europäische Rechenzentren in Kopenhagen, Frankfurt, Amsterdam, Hamburg und Oslo.	Cloudflare ist ein Content-Delivery-Network (CDN)- und Cybersicherheitsunternehmen, das Website-Optimierung, DDoS-Schutz und andere Sicherheitsfunktionen bereitstellt, um die Leistung des Systems zu verbessern und vor Online-Bedrohungen zu schützen. Cloudflare bietet eine Reihe von Sicherheitsfunktionen, um das System vor Cyberangriffen zu schützen. Die Firewall von Cloudflare blockiert böswilligen Datenverkehr, während das SSL-Zertifikat den Webdatenverkehr verschlüsselt, um Benutzerdaten zu schützen. Die DNS-Dienste von Cloudflare tragen zum Schutz vor DNS-Angriffen bei, während die Browser-Isolationstechnologie zum Schutz vor Malware und anderen Bedrohungen beiträgt.

Bei Inkrafttreten der Bestimmungen hat der Datenverantwortliche die Inanspruchnahme der oben genannten Unterauftragsverarbeiter für die beschriebene Verarbeitungstätigkeit genehmigt. Der Datenverarbeiter darf – ohne die schriftliche Zustimmung des Datenverantwortlichen – keinen Unterauftragsverarbeiter für eine andere als die beschriebene und vereinbarte Verarbeitungstätigkeit einsetzen oder einen anderen Unterauftragsverarbeiter für diese Verarbeitungstätigkeit einsetzen.

Im Falle der Übermittlung personenbezogener Daten in Drittländer, in denen der Unterauftragsverarbeiter nicht nach dem EU-U.S. Data Privacy Framework zertifiziert ist, erfolgt die Übermittlung stattdessen auf Grundlage der Standardvertragsklauseln (SCC) der Europäischen Kommission

Personenbezogene Daten dürfen nur an den im obigen Schema angegebenen Orten sowie an den folgenden Adressen über den Datenverarbeiter gespeichert werden:

- Sunekaer 9 | DK-5471 Soendersoe
- Anderupvej 16 | DK-5270 Odense N

B.2. Hinweis zur Genehmigung von Unterauftragsverarbeitern

Der Datenverarbeiter muss den Antrag auf eine spezifische Zustimmung mindestens zwei Monate vor dem Einsatz des betreffenden Unterauftragsverarbeiters stellen.

ANHANG C WEISUNGEN ZUR VERARBEITUNG PERSONENBEZOGENER DATEN

C.1. Gegenstand der Verarbeitung/Weisungen

Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen erfolgt, indem der Datenverarbeiter Aufgaben gemäß der Hauptvereinbarung ausführt.

Der Datenverarbeiter muss die personenbezogenen Daten im Auftrag des Datenverantwortlichen gemäß den schriftlichen Weisungen des Datenverantwortlichen verarbeiten und darf sie nur zu dem in der Datenverarbeitungsvereinbarung festgelegten Zweck verarbeiten. Die Anweisungen umfassen Folgendes:

- Lieferung des Systems
- Erhebung, Speicherung und Verarbeitung der personenbezogenen Daten gemäß den Weisungen des Datenverantwortlichen und den geltenden Datenschutzgesetzen
- Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten durch geeignete technische und organisatorische Sicherheitsmaßnahmen
- Löschung oder Rückgabe der personenbezogenen Daten gemäß den Weisungen des Datenverantwortlichen bei Ablauf der Datenverarbeitungsvereinbarung
- Meldung von Sicherheitsverletzungen, unbefugtem Zugriff oder Offenlegung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Entdeckung an den Datenverantwortlichen
- Anonymisierung von Informationen zu folgenden Zwecken:
    - Entwicklung, Optimierung und Analyse des Systems
    - Erstellung und Veröffentlichung von Statistiken, Berichten und Berechnungen im Zusammenhang mit dem System
    - Weitergabe und Verkauf anonymisierter Daten an Dritte

  Der Datenverarbeiter garantiert, dass Daten ausschließlich in vollständiger und unwiderruflich anonymisierter Form verarbeitet werden, wodurch es weder für den Datenverarbeiter noch für andere Personen möglich sein wird, abzuleiten, welche Daten mit welchen physischen Personen in Verbindung stehen.

C.2. Verarbeitungssicherheit

Der Datenverarbeiter muss die folgenden Maßnahmen umsetzen, die mit dem Datenverantwortlichen vereinbart wurden:

Allgemeine Sicherheitsmaßnahmen

Der Datenverarbeiter muss ein formelles, gut implementiertes und professionelles Managementsystem für Datensicherheit unterhalten, das auf gesetzlichen Anforderungen und guter Datenverarbeitungspraxis basiert. Der Datenverarbeiter muss interne Richtlinien und Vorschriften festlegen und umsetzen, die angemessen sind und die tatsächlichen Verhältnisse widerspiegeln. Darüber hinaus muss der Datenverarbeiter Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen unterhalten, die der Datenverarbeiter zur Sicherung der personenbezogenen Daten implementiert hat. Der Datenverarbeiter gewährleistet:

- Penetrationstests (Schwachstellenscans) sowohl auf der LAN- als auch auf der WAN-Seite
- systematisches Patchen/Aktualisierung der Software (Betriebssystem usw.)
- Überwachung kritischer Systeme, die Benachrichtigungen senden, wenn ein oder mehrere Systeme nicht wie erwartet funktionieren
- unabhängige Backup-Lösungen
- die Rechenzentren sind sicher verschlossen – und es gibt eine Kameraüberwachung
- automatische Feuerlöschanlagen sind in den Rechenzentren aktiviert
- redundante Kühlsysteme sind in unseren Rechenzentren eingerichtet
- zwei unabhängige Notstromsysteme stehen zur Verfügung
- Verschlüsselung
- Umsetzung der IT-Sicherheitsrichtlinie
- Netzwerküberwachung
- Spiegelung von Daten
- Support rund um die Uhr
- Security Incident Management (Störungsabläufe)
- Protokollierung der Netzwerkaktivitäten
- Trennung von Konto und Berechtigungen

Umgang mit personenbezogenen Daten

Dokumente und Daten (einschließlich mobiler Speichermedien), die personenbezogenen Daten enthalten, werden so verarbeitet, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Robustheit gewahrt werden, um sicherzustellen, dass sie nicht verloren gehen oder in die falschen Hände geraten und um die nachteiligen Folgen zu verhindern, die solche Verletzungen für betroffene Personen haben können.

Unterweisung der Mitarbeiter usw.

Der Datenverarbeiter stellt sicher, dass Mitarbeiter und etwaige Kooperationspartner ständig über den Zweck der Datenverarbeitung, Richtlinien, Arbeitsverfahren und ihre Geheimhaltungspflicht informiert sind und über ausreichende Schulungen und Anweisungen verfügen.

Zugriffskontrolle und Verwaltung des Benutzerzugriffs
Als Benutzer mit Zugriff auf die personenbezogenen Daten des Datenverantwortlichen dürfen nur Mitarbeiter eingerichtet werden, die einen arbeitsbedingten Bedarf haben, personenbezogene Daten im Zusammenhang mit der Hauptvereinbarung zu verarbeiten. Auf die personenbezogenen Daten dürfen nur diejenigen Personen zugreifen, die von der bevollmächtigten Person dazu befugt sind. Der Datenverarbeiter muss Berechtigungen (einschließlich Zugang) für Benutzer, die keinen arbeitsbedingten Berechtigungsbedarf mehr haben, unverzüglich aufheben.

Es wird eine Liste der autorisierten Mitarbeiter geführt, aus der hervorgeht, für welche Art von Zugriff die Autorisierung gilt. Die Liste der autorisierten Mitarbeiter wird gemäß guter Datenverarbeitungspraxis regelmäßig aktualisiert. Wenn der Datenverantwortliche die Liste anfordert, muss die Liste unverzüglich zur Verfügung gestellt werden.

Bei Beendigung der Leistung wird der Zugriff der Mitarbeiter gesperrt.

Der Datenverarbeiter muss sichere Identifizierungs- und Autorisierungstechnologien verwenden, wie beispielsweise Passwörter, Biometrie oder Ähnliches. Die verwendeten Authentifizierungsmethoden müssen den neuesten Leitlinien der dänischen Agentur für Digitalisierung und bewährten Verfahren in diesem Bereich entsprechen.

Kontrolle abgelehnter Zugriffsversuche
Basierend auf einem risikobasierten Ansatz registriert der Datenverarbeiter abgelehnte Zugriffsversuche und blockiert weitere Versuche nach einer festgelegten Anzahl aufeinanderfolgender abgelehnter Zugriffsversuche.

Der Datenverarbeiter muss auch Verfahren unterhalten, die eine zeitnahe Nachverfolgung aller abgelehnten Zugriffsversuche gewährleisten, wenn eine Nachverfolgung erforderlich ist, um Verletzungen der Sicherheit personenbezogener Daten und nachteilige Folgen für registrierte Personen zu verhindern.

Änderungsmanagement

Der Datenverarbeiter muss über formale Änderungsmanagementverfahren verfügen, um sicherzustellen, dass jede Änderung vor der Implementierung ordnungsgemäß autorisiert, getestet und genehmigt wird.

Betriebsunterbrechungen

Der Datenverarbeiter muss über dokumentierte Notfallverfahren verfügen, die im Falle von Betriebsunterbrechungen die Wiederherstellung der Dienste ohne ungerechtfertigte Ausfallzeiten gemäß der Hauptvereinbarung gewährleisten.

Externe Kommunikationsverbindungen

Der Datenverarbeiter verfügt über geeignete technische Maßnahmen zum Schutz von Systemen und Netzwerken sowie zur Begrenzung des Risikos eines unbefugten Zugriffs und/oder der Installation von Schadcodes.

Soweit dies nach geltendem Recht, guter Datenverarbeitungspraxis oder anderweitig laut Hauptvereinbarung erforderlich ist, wendet der Datenverarbeiter Verschlüsselungstechnologien und andere entsprechende Maßnahmen an.

Ad-hoc- und Heimarbeitsplätze

Wenn der Datenverarbeiter die Datenverarbeitung von Ad-hoc- und/oder Heimarbeitsplätzen aus ausführt, so hat er dafür zu sorgen, dass diese die Sicherheitsanforderungen dieser Datenverarbeitungsvereinbarung mit Anhängen, die Gesetzgebung im Allgemeinen und die diesbezüglichen Leitlinien der dänischen Datenschutzbehörde erfüllen.

Der Datenverarbeiter muss unter anderem Folgendes erfüllen und dokumentieren können:

- eine Beschreibung der verschlüsselten Verbindung, die zwischen dem Ad-hoc-Arbeitsplatz und dem Netzwerk des Datenverarbeiters/Datenverantwortlichen genutzt wird
- die internen Anweisungen des Datenverarbeiters an seine eigenen Mitarbeiter in Bezug auf Ad-hoc- und Heimarbeitsplätze

Darüber hinaus muss der Datenverarbeiter, sofern dies technisch möglich ist, eine 2-Faktor-Authentifizierung verwenden.

Entsorgung von Geräten

Der Datenverarbeiter muss über formelle Prozesse verfügen, um sicherzustellen, dass personenbezogene Daten vor der Entsorgung elektronischer Geräte effektiv gelöscht werden.

C.3 Unterstützung des Datenverantwortlichen

Der Datenverarbeiter unterstützt den Datenverantwortlichen nach Möglichkeit gemäß den Bestimmungen 9.1 und 9.2.

Dies bedeutet, dass der Datenverarbeiter unter Berücksichtigung der Art der Verarbeitung den Datenverantwortlichen in Verbindung damit unterstützen muss, dass der Datenverantwortliche die Einhaltung von Folgendem sicherstellen muss:

a. die Verpflichtung, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein den mit der Verarbeitung verbundenen Risiken angemessenes Sicherheitsniveau zu gewährleisten
b. die Verpflichtung, Verletzungen der Sicherheit personenbezogener Daten der Aufsichtsbehörde (der dänischen Datenschutzbehörde) unverzüglich und, wenn möglich, nicht später als 72 Stunden, nachdem der Datenverantwortliche von der Verletzung Kenntnis erlangt hat, zu melden, es sei denn, es ist unwahrscheinlich, dass die Verletzung der Sicherheit personenbezogener Daten ein Risiko für die Rechte oder Freiheiten natürlicher Personen birgt
c. die Verpflichtung, die betroffene(n) Person(en) unverzüglich über eine Verletzung der Sicherheit personenbezogener Daten zu informieren, wenn eine solche Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt
d. die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung, wenn eine Art der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt
e. die Verpflichtung, vor der Verarbeitung die Aufsichtsbehörde (die dänische Datenschutzbehörde) zu konsultieren, wenn eine Folgenabschätzung in Bezug auf den Datenschutz zeigt, dass die Verarbeitung zu einem hohen Risiko führen wird, wenn der Datenverantwortliche keine Maßnahmen zur Begrenzung des Risikos trifft

C.4 Aufbewahrungsfrist/Löschroutine

Die personenbezogenen Daten werden vom Datenverarbeiter gespeichert, bis der Datenverantwortliche die Löschung oder Rückgabe der Daten verlangt oder solange eine sachliche Grundlage für die Speicherung besteht.

Bei Beendigung der Dienstleistungen zur Verarbeitung personenbezogener Daten muss der Datenverarbeiter die personenbezogenen Daten gemäß Bestimmung 11.1 entweder löschen oder zurückgeben, es sei denn, der Datenverantwortliche hat – nach Unterzeichnung dieser Bestimmungen – seine ursprüngliche Wahl geändert.

Solche Änderungen sind zu dokumentieren und zusammen mit den Bestimmungen schriftlich, auch in elektronischer Form, festzuhalten.

C.5 Ort der Verarbeitung

Die Verarbeitung der unter die Bestimmungen fallenden personenbezogenen Daten darf ohne die vorherige schriftliche Zustimmung des Datenverantwortlichen nicht an anderen als den in Anhang B angegebenen Orten erfolgen.

C.6 Weisung zur Übermittlung personenbezogener Daten an Drittländer

Der Auftragsverarbeiter ist berechtigt, personenbezogene Daten in Drittländer zu übermitteln, soweit dies aus Anhang B hervorgeht.

Im Falle der Übermittlung personenbezogener Daten in Drittländer ist die Rechtsgrundlage für die Übermittlung:

- das EU-U.S. Data Privacy Framework (DPF), sofern der Unterauftragsverarbeiter entsprechend zertifiziert ist, oder
- die Standardvertragsklauseln (SCC) der Europäischen Kommission, sofern der Unterauftragsverarbeiter nicht nach dem DPF zertifiziert ist.

Der Auftragsverarbeiter hat sicherzustellen, dass gemäß der Datenschutz-Grundverordnung geeignete Schutzmaßnahmen für die Übermittlung getroffen werden.

C.7 Verfahren für die Audits des Datenverantwortlichen, einschließlich Inspektionen, im Zusammenhang mit der Verarbeitung personenbezogener Daten, die dem Datenverarbeiter anvertraut wurden

Der Datenverarbeiter muss seine internen Sicherheitsmaßnahmen mindestens einmal jährlich überprüfen.

Der Datenverarbeiter muss auf eigene Kosten eine Erklärung oder eine andere Form der Prüfung von einem unabhängigen Dritten über die Einhaltung dieser Datenverarbeitungsvereinbarung mit Anhängen durch den Datenverarbeiter einholen.

Die Erklärung bzw. das Ergebnis der Prüfung wird schnellstmöglich nach Einholung zur Information an den Datenverantwortliche gesendet.

Der Datenverantwortliche oder ein Vertreter des Datenverantwortlichen hat auch Zugang, um Inspektionen, einschließlich physischer Inspektionen, der Räumlichkeiten durchzuführen, von denen aus der Datenverarbeiter personenbezogene Daten verarbeitet, einschließlich physischer Räumlichkeiten und

Systeme, die für oder im Zusammenhang mit der Verarbeitung genutzt werden. Solche Inspektionen können durchgeführt werden, wenn der Datenverantwortliche dies für erforderlich hält.

C.8 Aufsicht über Unterauftragsverarbeiter

Der Auftragsverarbeiter führt laufende Risikobewertungen seiner Unterauftragsverarbeiter durch und nimmt Folgemaßnahmen in Form von Besprechungen, Inspektionen, Einholung und Bewertung von Prüfberichten oder gleichwertiger Dokumentation vor. Der Auftragsverarbeiter dokumentiert die Aufsichtsaktivitäten und stellt diese dem Verantwortlichen auf Anfrage zur Verfügung.

ANHANG D REGELUNG ANDERER ANGELEGENHEITEN DURCH DIE PARTEIEN

D.1. Benachrichtigung über eine Verletzung der Sicherheit personenbezogener Daten

Gemäß Punkt 10 der Datenverarbeitungsvereinbarung muss der Datenverarbeiter den Datenverantwortlichen unverzüglich benachrichtigen, nachdem er Kenntnis davon erlangt hat, dass eine Verletzung der Sicherheit personenbezogener Daten aufgetreten ist. Die Benachrichtigung des Datenverarbeiters an den Datenverantwortlichen muss nach Möglichkeit spätestens 12 Stunden, nachdem dieser von der Verletzung Kenntnis erlangt hat, erfolgen.

Die Benachrichtigung des Datenverarbeiters an den Datenverantwortlichen muss Informationen über Folgendes enthalten:

- Beschreibung der Verletzung und deren Ursache
- Datum und Uhrzeit des Beginns der Verletzung
- Datum und Uhrzeit der Entdeckung der Verletzung
- Gesamtdauer der Verletzung
- Auflistung der Art der von der Verletzung betroffenen personenbezogenen Daten (z. B. Name, CPR-Nummer, Finanzinformationen usw.)
- Anzahl der registrierten Personen, die von der Verletzung betroffen sind
- Beschreibung der wahrscheinlichen Folgen/nachteiligen Auswirkungen der Verletzung
- Beschreibung der Maßnahmen, die ergriffen wurden, um die Verletzung zu stoppen oder einzuschränken, einschließlich Datum und Uhrzeit
- Informationen darüber, ob die betroffenen registrierten Personen über die Verletzung informiert wurden und wie die gegebenenfalls geschehen ist
- Name *und* Kontaktdaten des Datenschutzberaters oder einer anderen Anlaufstelle, wo weitere Informationen eingeholt werden können
- etwaige andere Informationen, die erforderlich sind, damit der Datenverantwortliche seiner Verpflichtung nachkommen kann, die Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden; vgl. die Datenschutzverordnung Art. 33

Der Datenverarbeiter muss den Datenverantwortlichen auch bei der Bereitstellung der oben genannten Informationen im Zusammenhang mit der Verpflichtung des Datenverantwortlichen unterstützen, Verletzungen der Sicherheit personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden.

ENDE