Universität Zürich[UZH]

EU- Standardvertragsklauseln Auftragsverarbeiter (K(2010) 593) vom Juli 2018

Standardvertragsklauseln gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur): **Universität Zürich (UZH), [Name Organisationseinheit]**
Anschrift: ……
Tel.: ……Fax ....
E-Mail: .....
Weitere Angaben zur Identifizierung der Organisation
.....

(„Daten**exporteur**“)

und

Bezeichnung der Organisation (Datenimporteur): .....……
Anschrift: ……
Tel.: ……Fax ....
E-Mail: .....
Weitere Angaben zur Identifizierung der Organisation
.....

(„Daten**importeur**“)

(die „Partei“, wenn eine dieser Organisationen gemeint ist, die „Parteien“, wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1
Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

b) der „Datenexporteur“ ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur“ ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter“ ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs

personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2
Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3
Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4
Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5
Pflichten des Datenimporteurs ([1])

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung

[1] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6
Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7
Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8
Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9
Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: Schweizer Recht / Recht des Kantons Zürich. Soweit nicht anders definiert, haben alle Begriffe die gleiche Bedeutung wie im Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich vom 12. Februar 2007 sowie in der Verordnung über die Information und den Datenschutz (IDV) vom 28. Mai 2008.

Zusätzlich zu diesen Klauseln müssen bei einem Datenexport folgende Standarddokumente vom Datenimporteur angenommen werden:

1. Allgemeine Geschäftsbedingungen der Universität Zürich bei Auslagerung von Informatikleistungen (AGB DS Auslagerung IT UZH) vom Mai 2016, für den Fall, dass der Datenexporteur Informatikleistungen vom Datenimporteur in Anspruch nimmt; oder alternativ

2. Allgemeine Geschäftsbedingungen der Universität Zürich bei einer Datenbearbeitung durch Dritte (AGB DS Bearbeitung Dritte UZH) vom Mai 2016, für den Fall, dass der Datenexporteur keine Informatikleistungen von Dritten bezieht; und
3. Geheimhaltungserklärung der Universität Zürich vom Mai 2016, und
4. Allgemeine Geschäftsbedingungen der SIK für IKT-Leistungen, Ausgabe Januar 2015 (AGB für IKT-Leistungen, Ausgabe Januar 2015).

Klausel 10
Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11
Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss ([2]). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: Schweizer Recht / Recht des Kantons Zürich

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12
Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

[2] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Für den Datenexporteur:

Name ausgeschrieben.....

Funktion: ….....

Anschrift: .....

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Für den Datenimporteur:

Name ausgeschrieben.....

Funktion: ….....

Anschrift: .....

Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Anhang 1

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden

Die Mitgliedstaaten können entsprechend den nationalen Verfahren Zusatzangaben, die in diesem Anhang enthalten sein müssen, ergänzen

Datenexporteur
Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):

.....
.....
.....

Datenimporteur
Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):

.....
.....
.....

Betroffene Personen
Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):
.....
.....
.....

Kategorien von Daten
Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):
.....
.....
.....

Besondere Datenkategorien (falls zutreffend)
Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):

.....
.....
.....

Verarbeitung
Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):
.....
.....
.....

DATENEXPORTEUR
Name: ……
Unterschrift des/der Bevollmächtigten: .....

DATENIMPORTEUR
Name: ……
Unterschrift des/der Bevollmächtigten: .....

Anhang 2

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

Zutrittskontrolle: Massnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird	▪ Alarmsystem, welches beim Nichtschliessen von Zugängen zum Rechenzentrum oder anderen Räumlichkeiten reagiert. ▪ Überwachung des Rechenzentrums oder anderer Räumlichkeiten mittels Videokameras. ▪ Führen eines Besucherlogs für Zugänge zum Rechenzentrum oder zu solchen Räumlichkeiten oder Anlagen, in / mit denen eine Datenverarbeitung stattfindet. Die Logs müssen jederzeit einsehbar sein. ▪ Führen einer Zutrittsliste, welche alle berechtigten Personen aufführt, die Zutritt zu Räumlichkeiten oder Anlagen haben, in / mit denen eine Datenverarbeitung stattfindet. ▪ Offenlegung auf Anfrage der UZH mittels entsprechender Dokumentation, wie der Prozess zur Verwaltung von Zutrittsberechtigten sichergestellt wird (Registration, Mutation, Löschung).
Zugangskontrolle: Massnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird	▪ Einsatz eines Perimeter-Schutzes mittels Firewalls und mehrstufigen Virenschutzsystemen (sowohl auf Gateways, Server und auf Arbeitsplatzsystemen). ▪ Verbindliche Vorgaben zum Einsatz von Passwörtern. ▪ Sperren des System bei mehreren ungültigen Anmeldeversuchen. ▪ Ausschliessliche Verwendung von persönlichen Benutzerkonten (keine Gruppenkonten).

Zugriffskontrolle: Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können	▪ Definition und Einsatz eines Berechtigungskonzepte für Applikationen, Speichersysteme, Datenbanken und andere Systemen. ▪ Überwachen der Zugriffe und Sicherstellen der Protokollierung von Zugriffen. ▪ Verbindliche Vorgaben und Prozesse zur Löschung von Daten und zur Ausserbetriebnahme von Systemen. Offenlegung der Vorgaben und Prozesse auf Anfrage der UZH. ▪ Verbindliche Vorgaben zur Nutzung von Fernwartung und Zugriffen von externen Dritten. Offenlegung der Vorgaben auf Anfrage der UZH. ▪ Starke Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren des Datenimporteur resp. durch den Unterauftragsverarbeiter. ▪ Rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte. ▪ Implementierung eines Least Privilege Model (Nutzer bzw. Administratoren des Datenimporteurs resp. des Unterauftragsverarbeiters sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen). ▪ Vier-Augen-Prinzip für kritische Administrationstätigkeiten.
Weitergabekontrolle: Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist	▪ Einsatz von Verschlüsselungsmechanismen und/oder elektronischen Signaturen bei der Übertragung von elektronischen Informationen. Offenlegung der Verschlüsselungsmechanismen und der Schlüsselstärke auf Anfrage der UZH.
Eingabekontrolle: Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	▪ Definition und Einsatz von Mechanismen zur Protokollierung von Datenveränderungen und von Datenlöschungen resp. Datenvernichtung. Offenlegung der Mechanismen auf Anfrage der UZH.
Auftragskontrolle: Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können	▪ Annahme der „AGB Datenbearbeitung durch Dritte“ resp. „AGB Auslagerung Informatikleistungen der UZH“ durch den Datenimporteur resp. durch den Unterauftragsverarbeiter. ▪ Unterzeichnung der „Geheimhaltungserklärung der UZH“ durch jeden Mitarbeitenden des Datenimporteurs resp. des Unterauftragsverarbeiters, der

	Zugriff auf Daten der UZH hat.
Verfügbarkeitskontrolle: Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind	▪ Sicherstellen des Brandschutzes (beispielsweise durch Brandschutzmelder und Brandschutzanlagen im Rechenzentrum). ▪ Schutz des Rechenzentrums und anderer Datenverarbeitungsanlagen vor Überhitzung und Feuchtigkeit. ▪ Einsatz einer unterbrechungsfreien Stromversorgung für die Datenverarbeitungsanlagen. ▪ Datensicherung über zwei Standorte verteilt (inklusive Backup). ▪ Offenlegung auf Anfrage der UZH, welche Systeme redundant oder georedundant aufgebaut sind. ▪ Offenlegung des Notfallplans mittels entsprechender Dokumentation auf Anfrage der UZH. ▪ Lieferung von Statistiken über die Verfügbarkeit der Dienstleistungen (inkl. Beinah-Ausfälle) in regelmässigen Abständen.
Zweckbindung / Trennungskontrolle: Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können	▪ Trennung von Produktions- und Testumgebung. bei geschäftskritischen Systemen der UZH. Offenlegung des Konzepts auf Anfrage der UZH mittels entsprechender Dokumentation. ▪ Sicherstellung einer durchgängigen Mandantenfähigkeit für alle Datenverarbeitungsanlagen.
Organisationskontrolle: Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird	▪ Offenlegung des IT Sicherheitskonzept (optimalerweise ISMS auf Basis ISO 27001) auf Anfrage der UZH mittels entsprechender Dokumentation. ▪ Offenlegung des „Security Incident Management“-Prozess auf Anfrage der UZH mittels entsprechender Dokumentation. ▪ Offenlegung des Risikomanagementprozesses auf Anfrage der UZH mittels entsprechender Dokumentation; hierbei müssen insbesondere diejenigen Risiken offengelegt werden, zu denen keine Massnahmen des Datenimporteurs umgesetzt werden oder die auf Dritte übertragen werden (beispielsweise an eine Versicherung).
Dienst-Kontrollmöglichkeiten für die UZH: Massnahmen, die gewährleisten, dass die Verfügbarkeit der genutzten Dienste des Datenimporteurs durch die UZH selbst überwacht werden können, soweit kein direkter Zugriff durch den Nutzer der UZH mehr auf Hard- / Software durch den Nutzer möglich ist.	▪ UZH muss die Möglichkeit haben, messbare Größen, wie im SLA vereinbart, zu überwachen.

Monitoring und Security Incident Management: Massnahmen, die gewährleisten, dass die Informationssicherheit im laufenden Betrieb aufrecht erhalten wird. Dazu gehören das Aufdecken und die Behandlung von Angriffen bzw. Sicherheitsvorfällen durch ein Sicherheitsmonitoring sowie die angemessene Reaktion auf entdeckte Sicherheitsvorfälle.	▪ 24/7umfassende Überwachung der ausgelagerten Dienste sowie zeitnahe Reaktion bei Angriffen bzw. Sicherheitsvorfällen ▪ Erfassung und Auswertung von Datenquellen (z.B. Systemstatus, fehlgeschlagene Authentisierungsversuche, etc.) ▪ 24/7-erreichbares, handlungsfähiges Team für „Security Incident Handling“ und „Trouble-Shooting“. ▪ Mitteilungspflichten des Datenimporteurs gegenüber der UZH zu Sicherheitsvorfällen oder Hinweise auf Sicherheitsvorfälle, die die betroffene Person(en) betreffen könnten. ▪ Geeignete Bereitstellung relevanter Logdaten durch den Datenimporteur. ▪ Logging und Monitoring der Aktivitäten von Administratoren. ▪ Einbindung der UZH in sicherheitsrelevante Vorfälle. ▪ Überwachung der Infrastruktur auf sicherheitsrelevante Vorfälle (beispielsweise mittels IDS, IPS oder „Security Incident and Event Management“ - SIEM).
Notfallmanagement: Massnahmen, die vorbeugenden Schutz gegen mögliche Gefährdungen gewährleisten.	▪ Der Datenimporteur muss ein Notfallmanagement aufsetzen und betreiben. ▪ Der Datenimporteur muss der UZH die Priorisierung des Wiederanlaufs für die angebotenen Cloud-Dienste transparent machen. ▪ Regelmässige Notfall-Übungen (z.B. zum Ausfall eines Cloud Computing Standorts) ▪ Nachweis des Datenimporteurs, dass sein Notfallmanagement auf einem international anerkannten Standard wie z.B. ISO ISO 22301 resp. 27031 basiert (z.B. anhand Notfallvorsorgekonzept und Notfallhandbuch).
Interoperabilität und Portabilität: Massnahmen, die gewährleisten, dass zwei oder mehr unabhängige ausgelagerte Computing Plattformen zusammenarbeiten, ohne dass gesonderte Absprachen zwischen den Plattformen notwendig sind. Hierzu ist die Nutzung gemeinsamer Standards die Grundlage. Im Weiteren ist die Portabilität bzw. Plattformunabhängigkeit zu berücksichtigen um z.B. im Falle eines Konkurses eines Leistungserbringer die gesamte Plattform portieren zu können.	▪ Standardisierte oder offen gelegte Schnittstellen (API und Protokolle). ▪ Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen und ggf. Offenlegung der damit verbundenen Kosten (SaaS).

Sicherheitsprüfung und Nachweis: Massnahmen, die gewährleisten, dass das Informationssicherheitsmanagement des Datenimporteurs einer regelmäßigen Überprüfung der etablierten Sicherheitsmaßnahmen sowie des Informationssicherheits-Prozesses unterzogen werden	▪ Der Datenimporteur muss gegenüber der UZH regelmäßig über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle, die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests berichten. ▪ Regelmässiges Durchführen von Penetrationstests. ▪ Regelmässiges durchführen von Penetrationstests bei Unterauftragsverarbeitern. ▪ Regelmäßige und unabhängige Sicherheitsrevisionen bei Unterauftragsverarbeitern. ▪ Einräumung des Rechts, vorangekündigt und mit einer Vorlaufzeit von 4 Wochen einen Sicherheitsaudit zu den erbrachten Dienstleistungen und damit im Zusammenhang stehenden Räumlichkeiten und Datenverarbeitungsanlagen durchzuführen.
Zusätze zur Vertragsgestaltung: Massnahmen die gewährleisten, dass die genauen Modalitäten der Nutzung der Dienste des Datenimporteurs geklärt sind. Darunter sind unter anderem die Klärung von Punkten wie Ansprechpartnern, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der Sicherheitsvorkehrungen, Umgang mit Daten von betroffenen Personen und Weitergabe von Informationen an Dritte zu verstehen.	▪ Offenlegung der Standorte des Datenimporteurs und der/des Unterauftragsverarbeiter(s) (Land, Region), an denen die personenbezogenen Daten der UZH gespeichert und verarbeitet werden. ▪ Offenlegung der/des durch den Datenimporteur eingesetzten Unterauftragsverarbeiter(s), der/die für die Erbringung des ausgelagerten Dienste erforderlich sind. ▪ Transparenz, welche Eingriffe der Datenimporteur und der/die Unterauftragsverarbeiter in personenbezogene Daten und Verfahren der UZH vornehmen dürfen. ▪ Regelmäßige Unterrichtung über Änderungen (z.B. neue oder abgekündigte Funktionen, neue Unterauftragsverarbeiter, andere Punkte, die für das SLA relevant sind). ▪ Transparenz, welche Software durch den Datenimporteuer für die Nutzung der Dienste auf Seiten der UZH installiert sowie über die daraus resultierenden Sicherheitserfordernisse/-risiken. ▪ Transparenz bezüglich staatlicher Eingriffs- und Einsichtsrechte, über gerichtlich festlegbare Einsichtsrechte Dritter und über Prüfpflichten zu gespeicherten Daten der UZH durch den Datenimporteuer an allen potenziellen Standorten. ▪ Darlegung der Rechts- und Besitzverhältnisse des Datenimporteurs sowie der Entscheidungsbefugnisse.

Zusätzlich müssen folgende Informationssicherheitsmassnahmen erfüllt werden, welche auf Seite 12 im „Leitfaden Bearbeitung im Auftrag“ des Datenschutzbeauftragten des Kantons Zürich (vgl. https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/veroeffentlichungen/leitfaeden_und_checklisten/_jcr_content/contentPar/publication_3/publicationitems/leitfaden_bearbeiten/download.spooler.download.1437547151704.pdf/Leitfaden_Bearbeiten_im_Auftrag.pdf) bei einer Bearbeitung von Informationen der UZH (Datenexporteur) durch einen Auftragsdatenbearbeiter (Datenimporteur) gefordert werden:

- Verschlüsselung des Transportwegs
  Authentisierung mittels Benutzer ID und Passwort
  Gewährleistung der Passwort-Sicherheit
  Verhinderung der Top-Risiken (OWASP) im Web
  Protokollierung der Datenänderungen
  Umsetzungsplanung gemäss ISO 27002
  Notfallplanung
  Backupkonzepte
  Kontrolle des IT-Betriebs
  Informationspflicht Auftraggeber (Schutzbedarf, Aufbewahrungsfristen)
  Informationspflicht Auftragnehmer (Methoden, Prozesse, Unterauftragnehmer, besondere Vorkommnisse)
  Mandantentrennung
- Portabilität
- Verschlüsselung der Datenablage, Keymanagement beim Auftraggeber
  Zwei-Faktor-Authentisierung
- ISMS ISO 27001 / BSI 100-1
  Vollständige Protokollierung

	Personendaten[1]	Besondere Personendaten
Auslagerung CH	■	■ ■ ■
Cloud CH	■ ■	■ ■ ■ ■
Auslagerung Ausland Cloud Ausland Angemessener Datenschutz[2]	■ ■	■ ■ ■ ■
Auslagerung Ausland Cloud Ausland Kein angemessener Datenschutz	■ ■ ■	■ ■ ■ ■

[1] Sachdaten: Der Schutzbedarf der Informationen und die daraus resultierenden organisatorischen und technischen Massnahmen werden im Einzelfall ermittelt.

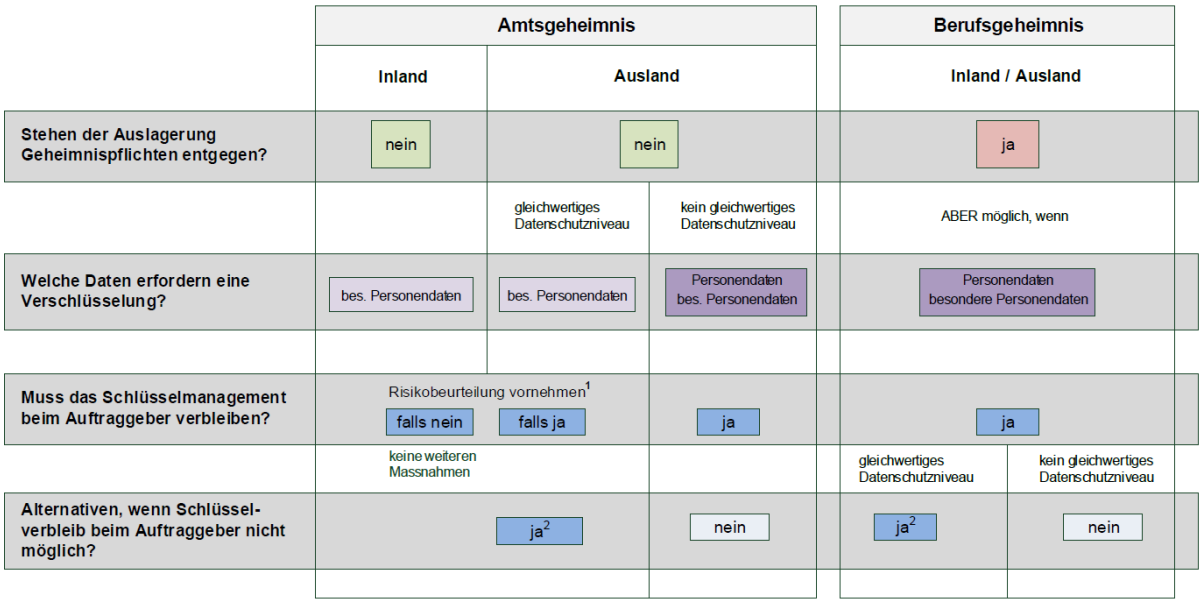
[2] Liste der Staaten mit angemessenem Datenschutzniveau

Die Liste der Staaten mit angemessenem Datenschutzniveau ist unter folgendem Link veröffentlicht: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf

Zur Verschlüsselung der Datenablage und zum Keymanagement müssen folgende Vorgaben und Alternativmöglichkeiten eingehalten werden, die der Datenschutzbeauftragte des Kantons Zürich im „Merkblatt Verschlüsselung der Datenablage im Rahmen der Auslagerung“ aufzeigt (vgl. https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/weitere_themen/outsourcing/_jcr_content/contentPar/downloadlist_3/downloaditems/verschl_sselung_der_.spooler.download.1529307028045.pdf/Verschluesselung_der_Datenablage_im_Rahmen_der_Auslagerung.pdf):

Verschlüsselung der Daten im Rahmen der Auslagerung –
unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten

dsb
datenschutzbeauftragter
kanton zürich



[1] **Kriterien Risikobeurteilung**
- Anzahl betroffene Personen
- Komplexität der Infrastruktur
- Risiko einer Persönlichkeitsverletzung je nach Art der Informationen
- Ort der Datenbearbeitung
- Umfang der Kontrollen durch Auftraggeber
- Umfang der Sicherheitsmassnahmen durch Auftragnehmer
- Aktuelle Risikolage

V 2.2 / Juni 2018

[2] **Vertragliche Absicherung**
Der Auftragnehmer muss sich vertraglich verpflichten, den Schlüssel nur auf explizite Anfrage und nach expliziter Einwilligung des Auftraggebers einzusetzen und auf die Daten zuzugreifen.
Conditio sine qua non
Der Auftragnehmer darf Kenntnis der Daten erlangen, wenn dies für die Aufgabenerfüllung unabdingbar ist, beispielsweise bei der Wartung medizinischer Instrumente.
Einwilligung Betroffener
Eine Auslagerung ist auch möglich, wenn Betroffene in die Offenlegung der vom Berufsgeheimnis geschützten Daten einwilligen.

Datenschutz mit Qualität

BEISPIEL FÜR EINE ENTSCHÄDIGUNGSKLAUSEL (FAKULTATIV)

Haftung

Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist.

Die Entschädigung ist abhängig davon, dass

a) der Datenexporteur den Datenimporteur unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und

b) der Datenimporteur die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten ([3]).

[3] Der Absatz über die Haftung ist fakultativ.