Anlage Datenschutz

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien die sich aus der im Vertrag beschriebenen Datenverarbeitung ergeben.

§ 1 Gegenstand und Dauer der Datenverarbeitung

(1) Die einzelnen Tätigkeiten, die Dauer der Datenverarbeitung durch den Auftragnehmer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien betroffenen Personen werden im voranstehenden Teil des Vertrages (im Folgenden „Vertrag") konkretisiert.

(2) Änderungsvereinbarungen im Hinblick auf den Verarbeitungsgegenstand sowie Verfahrensänderungen bedürfen der Schriftform oder sind in einem dokumentierten elektronischen Format abzufassen.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

(1) **Art der Verarbeitung der Daten**:

☐ Erhebung Falls zutreffend: Bei der betroffenen Person ☐ Bei Dritten ☐
☐ Speicherung
☐ Übermittlung
☐ Löschung/Vernichtung
☐ Veränderung
☐ Sperrung
☐ Nutzung
☐ Prüfung, Wartung oder Bereitstellung automatisierter Verfahren oder Datenverarbeitungs-
anlagen durch andere Stellen im Auftrag, bei welchen ein Zugriff auf personenbezogene Daten oder Kundendaten nicht ausgeschlossen werden kann.
☐ …….

Im Übrigen gelten die Bestimmungen des Vertrages.

(2) **Zweck der Verarbeitung**

Die Daten werden zu den im Vertrag beschriebenen Zwecken verarbeitet (vgl. §§ __).

(3) **Art der personenbezogenen Daten**

☐ besondere Arten personenbezogener Daten (Art. 9 DSGVO)
☐ Kontaktdaten
☐ KYC-Daten
☐ Ausweisdokumente
☐ Log-in Daten
☐ Audit-Trails
☐ ……

(4) **Kategorien betroffener Personen**

- ☐ Kunden (natürliche Personen)
- ☐ Kundendaten juristischer Personen (Daten sog. Connected Parties)
- ☐ Beschäftigtendaten
- ☐ Lieferantendaten
- ☐ Interessenten
- ☐ ……..

§ 3 Weisungsbefugnisse sowie Rechte und Pflichten des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Auftrag und nach Weisung des Auftraggebers.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen grundsätzlich schriftlich oder in einem dokumentierten elektronischen Format. Etwaige mündliche Weisungen werden unverzüglich schriftlich oder in einem dokumentierten elektronischen Format bestätigt.

(3) Wesentliche Änderungen im Verfahrensablauf beim Auftragnehmer sind vorab mit dem Auftraggeber abzustimmen und bedürfen der Schriftform oder sind in einem dokumentierten elektronischen Format abzufassen.

(4) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung sowie regelmäßig in angemessener Weise von der Einhaltung der Vorschriften über Datenschutz und Datensicherheit, der Einhaltung der beim Auftraggeber getroffenen technisch und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Die Prüfung erfolgt grundsätzlich nach Terminvereinbarung und kann auch durch vom Auftraggeber beauftragte Dritte erfolgen. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der vertraglichen und gesetzlichen Pflichten zur Verfügung stellen. Das umfasst die unverzügliche Beantwortung von Auskunftsanfragen sowie die Ermöglichung einer Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme. Zudem ist der Auftraggeber zu einer Überprüfung – einschließlich Inspektionen – vor Ort berechtigt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen gem. Art. 12 bis 22 DSGVO verantwortlich.

§ 4 [derzeit unbesetzt]

§ 5 Datenschutzbeauftrage

(1) Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz

_____

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Falls die Datenverarbeitung in Ländern erfolgt, in denen die Benennung eines Datenschutzbeauftragten nicht verbindlich ist oder kein Datenschutzbeauftragter benannt wurde, sind die Kontaktdaten der für die Einhaltung von Datenschutzvorschriften verantwortlichen Person dem Verantwortlichen mitzuteilen.

(2) Der Datenschutzbeauftragte des Auftraggebers ist unter

HSBC Continental Europe S.A., Germany, Datenschutzbeauftragter, Hansaallee 3, 40549 Düsseldorf, Telefon: 0211-910-2006, Fax: 0211–910-9-2125, E-Mailadresse: datenschutz@hsbc.de erreichbar.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung des Datenschutzbeauftragten bzw. der für die Einhaltung von Datenschutzvorschriften verantwortlichen Person sind dem Vertragspartner unverzüglich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

§ 6 Allgemeine Plichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation -, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). Falls eine solche Verpflichtung besteht, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Drittstaat statt, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Jede Verarbeitung in anderen Ländern bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

(3) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Zustimmung des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Kopien oder Duplikate, die zur Erfüllung der vereinbarten Dienstleistung erforderlich sind (z.B. Duplizieren von Datenbeständen für die Verlustsicherung, Erstellung von Log-Files, Anlegen von Zwischendateien und Arbeitsbereichen, etc.).

(4) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies verlangt und berechtigte Interessen des Auftragnehmers dieser Weisung nicht entgegenstehen.

(5) Nach Abschluss der Erbringung der Verarbeitungsleistung wird der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten entweder löschen oder zurückgeben.

(6) Die physische Vernichtung von Dokumenten und Datenträgern hat – sofern keine andere Weisung vorliegt - mindestens nach DIN 66399 Sicherheitsstufe 3 oder in ihrer Entsprechung und Wirkung nach DIN EN 15713 zu erfolgen. Erfolgt eine Datenlöschung beim Auftragnehmer, hat der Auftragnehmer sämtliche löschbaren elektronischen Datenträger, die Daten des Auftraggebers enthalten, datenschutzgerecht und nicht wieder herstellbar zu löschen. Daten in Datenbanksystemen sind so aus der logischen Struktur zu löschen, dass die Löschung nicht rückgängig gemacht werden kann. Der Auftragnehmer ist verpflichtet, technisch oder organisatorisch sicherzustellen, dass die Daten auch tatsächlich gelöscht werden. Hierüber hat der dem Auftraggeber auf Nachfrage einen Nachweis zu erbringen.

(7) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, falls er der Auffassung ist, dass eine vom Auftraggeber erteilte Weisung gegen gesetzliche Vorschriften verstößt. Er darf die Verarbeitung so lange aussetzen, bis der Auftraggeber die Weisung bestätigt.

(8) Der Auftragnehmer wird dem Auftraggeber die Prüfungen gem. § 3 (4) zeitnah (spätestens aber innerhalb von drei Wochen nach Anfrage) ermöglichen und an diesen unterstützend mitwirken. Im

Vorfeld der Prüfung angefragte Dokumente und Nachweise werden unverzüglich zur Verfügung gestellt.

(9) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

(10) Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb sowie bei den Subunternehmern über die gesamte Abwicklung der Dienstleistungen. Das Ergebnis der Kontrollen ist zu dokumentieren und dem Auftraggeber nach Aufforderung zur Verfügung zu stellen, soweit sie die Verarbeitung der Daten des Auftraggebers betreffen.

(11) Weitere Pflichten des Auftragnehmers ergeben sich aus den nachfolgenden Regelungen.

§ 7 Mitwirkung bei der Geltendmachung der Betroffenenrechte

(1) Sofern Rechte von durch die Datenverarbeitung betroffenen Personen beim Auftragnehmer geltend gemacht werden, ist der Auftraggeber für die Wahrung dieser Rechte verantwortlich.

(2) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

(3) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung des Auftraggebers erteilen.

§ 8 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten sowie sonstige Informationspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber (per E-Mail an incident.management@hsbc.de) unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen.

(2) Sollten die Daten des Verantwortlichen beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über und das Eigentum an den Daten ausschließlich beim Auftraggeber liegt.

(3) Der Auftragnehmer ist nicht befugt, jegliche Art von Rechten an den Daten des Auftraggebers geltend zu machen. Dazu zählen zum Beispiel Eigentums-, Zurückbehaltungs- und Sicherungsrechte.

(4) Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der

Daten des Auftraggebers betrifft oder betreffen kann. Die im Prüfbericht festgestellten wesentlichen Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

(5) Dem Auftraggeber werden durch den Auftragnehmer die zusammenfassenden, relevanten Prüfberichte des Datenschutzbeauftragten des Auftragnehmers zur Verfügung gestellt, soweit sie die Verarbeitung der Daten des Auftraggebers betreffen oder betreffen können. Die im Prüfbericht festgestellten wesentlichen Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

(6) Die Absätze 1 bis 4 gelten entsprechend für Vorkommnisse bei Prozessen, die von Subunternehmern ausgeführt werden.

§ 9 Datengeheimnis / Bankgeheimnis / Fernmeldegeheimnis

(1) Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die personenbezogenen Daten, zu denen sie Zugang haben, ausschließlich auf Weisung verarbeiten, es sei denn, dass sie nach dem Recht der Europäischen Union oder dem Recht der Mitgliedsstaaten der Europäischen Union zur Verarbeitung verpflichtet sind.

(2) Da der Auftraggeber dem Bankgeheimnis unterliegt**,** gelten die Verpflichtungen für die Wahrung des Bankgeheimnisses auch für den Auftragnehmer. Er wird seine Subunternehmer entsprechend verpflichten. Die vom Auftragnehmer eingesetzten Personen und Personen von ihm beauftragter Subunternehmer sind zur absoluten Verschwiegenheit über alle kundenbezogenen Informationen zu verpflichten. Informationen über Kunden dürfen nur vom Auftraggeber selbst oder vom Auftragnehmer nach vorheriger schriftlicher Zustimmung des Auftraggebers weitergegeben werden, es sei denn, die Weitergabe ist gesetzlich vorgeschrieben.

(3) Die Verpflichtung nach Absatz 1 und 2 muss vor der erstmaligen Aufnahme der Tätigkeit für den Auftraggeber erfolgt sein und ist dem Auftraggeber auf Verlangen nachzuweisen. Die Verpflichtung zur Gewährleistung der Vertraulichkeit nach Absatz 1 und 2 gilt über die Beendigung dieses Vertrages hinaus.

(4) Der Auftragnehmer stellt sicher, dass mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befasste Personen und Personen von ihm beauftragter Subunternehmer im Hinblick auf die anwendbaren Datenschutzvorschriften geschult sind.

(5) Wirken Personen des Auftragnehmers und von ihm beauftragter Subunternehmer am technischen Vorgang der Erbringung von Telekommunikationsdiensten für den Verantwortlichen mit, so erstreckt sich diese Sorgfaltspflicht auch auf das Fernmeldegeheimnis nach § 3 Telekommunikations-Telemedien-Datenschutzgesetz oder einer entsprechenden anwendbaren gesetzlichen Bestimmung des betreffenden Rechtsraumes. Die Verpflichtung dieser Personen auf die Wahrung des Fernmeldegeheimnisses muss vor der erstmaligen Aufnahme der Tätigkeit für den Auftraggeber vorgenommen sein und ist dem Auftraggeber auf Verlangen nachzuweisen.

§ 10 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen

(1) Der Auftragnehmer gewährleistet für jede Datenverarbeitung im Auftrag des Auftraggebers ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen der Schutz der Rechte der betroffenen Personen sichergestellt ist.

(2) Zudem sichert der Auftragnehmer zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Auch zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden. Dies setzt eine Trennung (physisch oder logisch) und wechselseitige Abschirmung der für die jeweiligen Verarbeitungszwecke und für die jeweiligen Mandanten verarbeiteten Datenbestände voraus.

(3) Das **im Anhang „Datensicherheit" beschriebene Datenschutzkonzept** stellt die implementierten technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(4) Der Auftragnehmer sichert in seinem Verantwortungsbereich die dauerhafte Einhaltung der vereinbarten allgemeinen sowie technischen und organisatorischen Maßnahmen entsprechend Artikel 32 DSGVO zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(5) Der Auftragnehmer hat Verfahren zur regelmäßigen (mindestens jährlichen) Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung implementiert. Das Ergebnis der Prüfung samt vollständigem Auditbericht wird dem Auftraggeber unaufgefordert unverzüglich mitgeteilt.

(6) Der Auftragnehmer sichert zu, dass er bzw. seine Subunternehmer über die erforderliche Herrschaft über die Datenverarbeitungsanlagen verfügen, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden. Dies schließt etwaige Eigentums- oder Besitzrechte ein.

(7) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragnehmer unterreichtet den Auftraggeber unter Einbeziehung seines Datenschutzbeauftragten unverzüglich in dokumentierter Form (schriftlich, elektronisch) bei Änderungen der technischen und organisatorischen Sicherheitsmaßnahmen und bei sonstigen Änderungen, die zu einer Verringerung des Schutzniveaus führen.

(8) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

§ 11 Zulässigkeit der Begründung von Unterauftragsverhältnissen (weitere Auftragsverarbeiter) und Bedingungen für deren Einsatz

(1) Die Beauftragung eines weiteren Auftragsverarbeiters durch den Auftragnehmer (Subunternehmer) zur Erfüllung einer Leistungsverpflichtung aus dem Vertrag bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Mit der Bitte um Zustimmung hat Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitzuteilen. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber zur Verfügung zu stellen.

(2) Eine allgemeine Vorabzustimmung zur Beauftragung weiterer Subunternehmers im Sinne des Artikel 28 Abs. 2 DSGVO erfolgt grundsätzlich nicht. Sofern im Ausnahmefall eine solche allgemeine Zustimmung ausdrücklich und schriftlich vereinbart wird, informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch einzulegen. Zur Beurteilung, ob ein Einspruch durch den Auftraggeber geltend gemacht wird, stellt der Auftragnehmer dem Auftraggeber aussagekräftige Informationen über den Subunternehmer zur Verfügung. Wird Einspruch erhoben, muss der Einsatz des Subunternehmers unterbleiben.

(3) Nicht der Regelung nach Absatz 1 unterliegen solche Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen zum Beispiel Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(4) Subunternehmer, deren Einsatz zur Durchführung des vereinbarten Auftrages als weiter beauftragte Auftragsverarbeiter bei Abschluss des Vertrages nach Absatz 1 gebilligt sind, werden im Anhang „**Gebilligte Subunternehmer**" benannt. Hierbei sind für jeden Subunternehmer der Leistungsort und die beauftragte Leistung zu beschreiben.

(5) Die Verarbeitung der Daten durch einen gebilligten Subunternehmer ist erst dann zulässig, wenn der Subunternehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO unterzeichnet und die geeigneten Garantien nach Artikel 28 Abs. 1 DSGVO nachgewiesen hat.

(6) Der Auftragnehmer hat sicherzustellen, dass ein gebilligter Subunternehmer in gleicher Weise wie er selbst vertraglich verpflichtet wird. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(7) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden oder in einem dokumentierten elektronischen Format.

(8) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach § 9 und Art. 29 sowie Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(9) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

(10) Die Verarbeitung der personenbezogenen Daten durch einen gebilligten Subunternehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Drittstaat statt, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Jede Verarbeitung in anderen Ländern oder bei einer internationalen Organisation bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.
Die Übermittlung in ein Drittland oder an eine internationale Organisation darf im Falle einer Zustimmung nur erfolgen, wenn die besonderen Voraussetzungen des Kapitel V der DSGVO erfüllt sind, sofern der Auftragsnehmer nicht durch das Recht der Europäischen Union oder eines Mitgliedsstaats der Europäischen Union, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 12 Regelmäßige Prüfung des Angemessenheitsbeschlusses

(1) Erfolgt die Datenverarbeitung in einem Drittstaat, für den ein Angemessenheitsbeschluss der Europäischen Kommission im Sinne des Artikels 45 DSGVO vorliegt, so überprüfen der

Auftraggeber und der Auftragnehmer regelmäßig die Fortgeltung des Angemessenheitsbeschlusses[1].

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, sofern ihm bekannt wird, dass der Angemessenheitsbeschluss aufgehoben, geändert oder ausgesetzt wird bzw. wurde.

(3) Der Auftraggeber behält sich das Recht vor, die Verlagerung der Datenverarbeitung in einen Mitgliedstaat der Europäischen Union, in einen anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einen Drittstaat, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, zu verlangen, falls die Wirkung des Angemessenheitsbeschlusses gemäß Bericht nach Artikel 45 Abs. 3 Satz 2 in Verbindung mit Artikel 45 Abs. 5 DSGVO aufgehoben, geändert oder ausgesetzt wird bzw. wurde.

§ 13 Sonstige Verpflichtungen über das Vertragsende hinaus

(1) Dokumentationen, die dem Nachweis der ordnungsmäßigen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Verantwortlichen bei Vertragsende übergeben. Der Auftragnehmer hat im Regressfall dem Verantwortlichem auch nach Vertragsende die noch vorhandenen Dokumentationen zur Führung des Entlastungsbeweises bei einer eventuellen Schadensersatzforderung wegen behaupteter unzulässiger oder unrichtiger Datenverarbeitung zu überlassen.

(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus, zeitlich unbegrenzt Stillschweigen über die im Zusammenhang mit dem Auftrag bekannt gewordenen Daten und Sachverhalte zu wahren.

§ 14 Haftung

(1) Für den Ersatz von Schäden und Mehraufwendungen, die dem Auftraggeber wegen einer nach der DSGVO oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Verarbeitung personenbezogener Daten im Rahmen des Auftragsverhältnisses entstehen, ist der Auftragnehmer verantwortlich. Unzulässig in diesem Sinne meint insbesondere die Verarbeitung, welche von Vorschriften der DSGVO oder anderen Vorschriften über den Datenschutz oder den Weisungen des Verantwortlichen abweicht sowie die fehlerhafte Verarbeitung aufgrund von Prozessfehlern des Auftragnehmers. Der Auftragnehmer wird den Verantwortlichen von eventuellen Ansprüchen Dritter in diesem Zusammenhang freistellen.

(2) Im Übrigen gelten bezüglich der Haftung die Haftungsregelungen aus dem oben genannten Vertrag. Sollten keine Haftungsregelungen im oben genannten Vertrag vereinbart worden sein, so gelten die gesetzlichen Bestimmungen zur Haftung.

[1] Eine Liste ist hier verfügbar:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

(Vorname, Name Auftraggeber in Klarschrift)

(Ort, Datum)

(Unterschrift Auftraggeber)

(Vorname, Name Auftragnehmer in Klarschrift)

(Ort, Datum)

(Unterschrift Auftragnehmer)

Anhang „Datensicherheit"

-Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO-

Präambel

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 und Freiheiten natürlicher Personen, konkretisiert dieser Anhang nach Artikel 32 DSGVO, die getroffenen technischen und organisatorischen Schutzmaßnahmen, die sich aus der im Vertrag in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.

Diese Anlage findet Anwendung auf alle Verarbeitungen personenbezogener Daten des Auftraggebers durch den Auftragnehmer oder von ihm beauftrage Subunternehmer.

§ 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

(1a) Maßnahmen zur **Pseudonymisierung und Anonymisierung** personenbezogener Daten:

Hinweis:

Pseudonymisierung ist die Verarbeitung personenbezogene Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Existieren solche zusätzlichen Informationen nicht oder werden sie unwiderruflich gelöscht, so handelt es sich um eine Anonymisierung.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1b) Maßnahmen zur **Verschlüsselung** personenbezogener Daten:

Hinweis:

Verschlüsselung personenbezogener Daten ist eine gängige Möglichkeit diese gegen die Kenntnisnahme durch Unbefugte zu schützen.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1c) Maßnahmen zur **Sicherstellung der Vertraulichkeit auf Dauer**:

Hinweis:

Damit sind Maßnahmen gemeint, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz von unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Vertraulichkeit auf Dauer gewährleisten.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1d) Maßnahmen zur **Sicherstellung der Integrität auf Dauer**:

Hinweis:

Damit sind Maßnahmen gemeint, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz von unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sowie unbefugter Änderung. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Integrität auf Dauer gewährleisten.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1e) Maßnahmen zur **Sicherstellung der Verfügbarkeit auf Dauer**:

Hinweis:

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1f) Maßnahmen zur **Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer**:

Hinweis:

Hierzu gehören beispielsweise Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Verantwortlichen und den Auftragnehmer zu ergreifen sind (vgl. 2i). Aber auch eine kontinuierliche Überwachung der Systeme kann erforderlich sein.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1g) Maßnahmen zur raschen **Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall**:

Hinweis:

Zur Sicherstellung der Wiederherstellbarkeit erscheinen einerseits ausreichende Sicherungen denkbar, wie aber auch Maßnahmenpläne, die im Sinne von Katastrophen-Fall-Szenarien (ggf. auch Basis der Sicherungen) den laufenden Betrieb wiederherstellen können.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1h) Maßnahmen zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**:

Hinweis:

Maßnahmen, um insbesondere die hier geregelten Maßnahmen zur Datensicherheit laufend aktuell zu halten.

Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

Anhang "Gebilligte Subunternehmer"

Kurzbeschreibung der Tätigkeit:	Name der Firma:	Sitz der Firma, Ort der Daten-verarbeitung:	Datenschutzbeauftragter / für den Datenschutz verantwortliche Person (Vorname Name, Kontaktdaten):

Dieser Hinweis wurde zuletzt am 01. Juli 2025 aktualisiert.

Annex: Data Protection

Agreement on commissioned data processing pursuant to Article 28 GDPR

Preamble

This annex sets out in concrete terms the data protection obligations of the contracting parties arising from the commissioned data processing described in the agreement.

§ 1 Subject matter and duration of the commissioned data processing

(1) The individual activities, the duration of the data processing by the Supplier, the nature and purpose of the processing, the type of personal data, and the categories of persons affected are set out in detail in the above section of the agreement ('the Agreement').

(2) Changes in respect of the data to be processed and the method of processing must be recorded in writing or in a documented electronic format.

§ 2 Nature and purpose of the processing, type of personal data, and categories of data subjects

(1) **Type of processing**:

☐ Collection Where applicable: From the data subject☐ From a third party☐
☐ Storage
☐ Transfer
☐ Deletion/Destruction
☐ Amendment
☐ Blocking
☐ Use
☐ Review, maintenance, or provision of automated processes or data processing facilities is commissioned from other parties and there is a possibility that third parties may gain access to personal data or customer data via them.
☐ …….

In other respects, the provisions of the Agreement apply.

(2) **Purpose of the processing**

The data will be processed for the purposes described in the Agreement (see clauses __).

(3) **Type of personal data**

☐ Special categories of personal data (Art. 9 GDPR)
☐ Contact details
☐ KYC data
☐ Identification documents
☐ Log-in data
☐ Audit trails
☐ ……

(4) **Categories of data subjects**

- ☐ Customers (individuals)
- ☐ Customer data of legal entities (data of 'connected parties')
- ☐ Employee data
- ☐ Supplier data
- ☐ Prospective customers
- ☐ ……..

§ 3 HSBC's rights, duties, and authority to issue instructions

(1) The Supplier processes personal data of HSBC exclusively on behalf of and in accordance with the instructions of HSBC.

(2) HSBC issues all orders, part-orders, and instructions in writing or in a documented electronic format. If instructions are issued orally, they will be confirmed without undue delay in writing or in a documented electronic format.

(3) Material changes in the procedure used by the Supplier must be agreed with HSBC and must be recorded in writing or in a documented electronic format.

(4) HSBC is entitled to take reasonable steps to satisfy itself – both before processing begins and at regular intervals thereafter – that the Supplier is complying with the requirements concerning data protection and data security, with the technical and organisation measures put in place by HSBC, and with the undertakings given in this Agreement. Checks will generally be carried out by prior arrangement and may also be carried out by a third party instructed by HSBC. The Supplier shall provide HSBC with all the information required for proof of compliance with the contractual and statutory obligations. This includes responding immediately to requests for information and allowing inspection of the stored data and data processing programs. HSBC is also entitled to carry out checks – including inspections – at the Supplier's premises.

(5) HSBC shall inform the Supplier without undue delay if it discovers errors or irregularities when checking the work results.

(6) HSBC alone is responsible for judging the reliability of the processing pursuant to Art. 6 (1) GDPR and for protecting the rights of the data subjects pursuant to Art. 12 to 22 GDPR.

§ 4 [*intentionally left blank*]

§ 5 Data protection officer

(1) The Supplier shall, without undue delay, provide HSBC with the contact details (first name, last name, organisational unit, telephone) of its data protection officer. If the data processing is carried out in countries in which there is no mandatory requirement to appoint a data protection officer or if no data protection officer has been appointed, the contact details of the person with responsibility for compliance with the data protection requirements must be provided to the controller.

(2) HSBC's data protection officer can be reached at the following address:

HSBC Continental Europe S.A., Germany, Data protection officer, Hansaallee 3, 40549 Düsseldorf, Germany
Tel: +49 (0)211-910-2006, Fax: +49 (0)211-910–9-2125, Email address: datenschutz@hsbc.de.

(3) In the event of a change of data protection officer or person with responsibility for data protection, or if the data protection officer or person with responsibility for data protection is unable to carry

out his or her duties for a prolonged period, the name of their successors or deputies must be provided to the contract partner without undue delay in writing or electronically.

§ 6 General duties of the Supplier

(1) The Supplier shall not process personal data except in connection with the agreed arrangements and in accordance with the instructions of HSBC – including in relation to the transfer of personal data to a third country or an international organisation – unless it is obliged to do so by European Union law or the law of the member states to which the Supplier is subject (e.g. investigations by criminal prosecution or state security authorities). Where such an obligation exists, the Supplier shall inform HSBC of these legal requirements prior to processing, so far as the law concerned does not prohibit such notification on the grounds of important public interest.

(2) Personal data is processed by the Supplier exclusively in the Federal Republic of Germany, in a member state of the European Union, in another of the signatory states to the Treaty on the European Economic Area, or in a third country for which the European Commission has adopted an 'adequacy decision'.

Any processing in other countries requires the prior written consent of HSBC.

(3) The Supplier shall not use the personal data supplied by HSBC for processing for any other purpose, especially not for its own purposes. The Supplier shall not make any copies or duplicates of the personal data without the consent of HSBC. This prohibition does not apply to copies or duplicates that are necessary to perform the agreed service (e.g. duplicates of data records for back-up, creation of log files, creation of intermediate files and work areas, etc.).

(4) The Supplier must correct, delete or restrict the processing of personal data under this Agreement if this is demanded by HSBC and if there are no legitimate interests of the Supplier that oppose this instruction

(5) Once the processing has been completed, the Supplier will, at the discretion of HSBC, either delete or return all personal data.

(6) The physical destruction of documents and data storage media must – in the absence of any other instruction – as a minimum adhere to the standards of DIN 66399 Security Level 3. It may be carried out in accordance with DIN EN 15713 provided this is equivalent to DIN 66399 Security Level 3 in terms of its effect. If data is deleted by the Supplier, the Supplier must also erase all erasable electronic data storage media that contain data from HSBC. This must be done in a manner that is consistent with the provisions of data protection law and ensures that the data cannot be recovered. Data in database systems is to be irreversibly deleted from the logic structure. The Supplier is obliged to ensure by technical or organisational means that the data has actually been deleted. It must provide evidence of this to HSBC upon request.

(7) The Supplier will inform HSBC without undue delay if, in the Supplier's opinion, instructions issued by HSBC are in breach of statutory provisions. The supplier may suspend the processing until HSBC confirms the instruction.

(8) The Supplier will enable HSBC to carry out the audits provided for in clause 3 (4) as soon as possible (but within no more than three weeks of receiving the request) and will provide assistance. Any documents and evidence requested in advance of the audit will be supplied without undue delay.

(9) Data processing in a private dwelling (remote or home working by employees of the Supplier) is permitted only with the consent of HSBC. If the data is processed at a private dwelling, access to the dwelling by HSBC for monitoring purposes shall be contractually agreed. The provisions of Art. 32 GDPR must be complied with in such a case.

(10) The Supplier shall monitor compliance with the provisions of data protection legislation both within its own business and at any subcontractors, at every stage of the service provision. Results of the

checks are to be documented and provided to HSBC upon request, so far as they relate to the processing of HSBC's data.

(11) Further obligations of the Supplier are set out in the provisions below.

§ 7 Cooperation in the enforcement of data subjects' rights

(1) If persons whose data is being processed seek to enforce their rights against the Supplier, it is HSBC who is responsible for protecting such rights.

(2) The Supplier must cooperate with HSBC to the extent necessary to assist it in asserting the rights of data subjects pursuant to Art. 12 to 22 GDPR, in creating records of processing activities, and in carrying out the necessary data protection impact assessments, and must support HSBC as far as possible with appropriate technical and organisational measures.

(3) The Supplier must not disclose information about personal data obtained in connection with this Agreement to third parties or to data subjects without the prior written consent of HSBC.

§ 8 Duties of the Supplier to cooperate in the event of disruptions to the processing and personal data breaches, and other obligations to provide information

(1) The Supplier shall inform HSBC (by sending an e-mail to incident.management@hsbc.de) without undue delay of any disruptions or violations of data protection legislation or of the specifications of the job order by the Supplier or by the persons employed by the Supplier, and of any suspicion of data protection breaches or irregularities in the processing of personal data. This applies in particular to any reporting obligations of HSBC under Art. 33 and Art. 34 GDPR. The Supplier promises to provide all reasonable assistance to HSBC in the fulfilment of its duties under Art. 33 and 34 GDPR.

(2) The Supplier must inform HSBC immediately if data belonging to the controller but in the possession of the Supplier is at risk through seizure or distraint, through insolvency or composition proceedings or through other events or actions by third parties. The Supplier shall inform all relevant bodies in this context without undue delay that ownership of and control over the data rests exclusively with HSBC.

(3) The Supplier is not authorised to assert any other rights whatsoever relating to HSBC's data. This includes rights of ownership and retention, and security interests.

(4) If audits are carried out by the data protection supervisory authorities, the Supplier undertakes to notify HSBC of the outcome, so far as it relates to or could relate to the processing of HSBC's data. The Supplier must rectify any material errors identified in the audit report without undue delay and inform HSBC that it has done so.

(5) The Supplier must provide the relevant audit reports produced by the Supplier's data protection officer to HSBC, so far as they relate or could relate to the processing of HSBC's data. The Supplier must rectify any material errors identified in the audit report without undue delay and inform HSBC that it has done so.

(6) Paragraphs (1) to (4) apply *mutatis mutandis* to occurrences relating to processes carried out by subcontractors.

§ 9 Data protection, banking secrecy, telecommunications secrecy

(1) The Supplier shall ensure that the persons entrusted with the processing of personal data have given a confidentiality undertaking or are subject to an appropriate statutory duty to maintain confidentiality and that they process the personal data to which they have access solely in accordance with instructions, unless they are obliged to process it in accordance with the law of the European Union or the law of any member state of the European Union.

(2) Since HSBC is subject to banking secrecy, the requirements pertaining to the maintenance of banking secrecy also apply to the Supplier. The Supplier shall require its subcontractors to give an equivalent undertaking. The persons deployed by the Supplier and the persons deployed by subcontractors engaged by the Supplier must be bound to maintain absolute discretion in respect of all customer-related information. Information concerning customers may be disclosed only by HSBC itself or by the Supplier with the prior written consent of HSBC, unless disclosure is required by statute.

(3) The undertakings required under paragraphs (1) and (2) must have been given prior to the commencement of the activity for HSBC and evidence of this must be provided to HSBC upon request. The obligation to maintain confidentiality under paragraphs (1) and (2) extends beyond the term of this Agreement.

(4) The Supplier shall ensure that the persons deployed by the Supplier and the persons deployed by subcontractors engaged by the Supplier receive training in respect of the applicable data protection provisions.

(5) If persons deployed by the Supplier and persons deployed by the subcontractors engaged by the Supplier are involved in the technical processes for the provision of telecommunications service for the controller, this duty of care also extends to the telecommunications secrecy under section 3 of the German Telecommunications-Telemedia Data Protection Act (TTDSG) or an equivalent applicable statutory provision of the jurisdiction concerned. The undertaking to maintain telecommunications secrecy must have been given prior to the commencement of the activity for HSBC and evidence of this must be provided to HSBC upon request.

§ 10 Technical and organisational measures pursuant to Article 32 GDPR

(1) The Supplier guarantees that every data processing assignment commissioned by HSBC will be carried out with a level of protection that is appropriate for the risk to the rights and freedoms of the individuals whose data is being processed. Due regard shall be given to the objectives set out in Art. 32 (1) GDPR, such as the ability to ensure confidentiality, integrity, availability, and resilience of processing systems and services with regard to the nature, scope, context, and purpose of the processing, by employing appropriate technical and organisational measures to ensure that the rights of the data subjects are protected.

(2) The Supplier further guarantees that the data being processed on behalf of HSBC will be strictly segregated from other data. Data collected for different purposes must also be processed separately. This requires a separation (physical or logical) and reciprocal shielding of the data processed for each specific processing purpose and for each individual customer.

(3) The **data protection concept outlined in the 'Data Security' annex** describes in detail the technical and organisational measures that have been put in place to ensure a level of security appropriate to the identified risk and that take account of the aims of the protection, use the best available technology, and take particular account of the IT systems and processing methods used by the Supplier.

(4) Within its area of responsibility, the Supplier guarantees ongoing compliance with the agreed general, technical, and organisational measures in accordance with Article 32 GDPR. In particular, the Supplier will organise its internal operations in such a way that they meet the specific requirements of data protection.

(5) The Supplier has implemented methods for the regular (at least once a year) review, assessment, and evaluation of the effectiveness of the technical and organisational measures to guarantee data protection-compliant processing. The results of the review and the full audit report will be communicated to HSBC without undue delay, without being specifically requested.

(6) The Supplier guarantees that it or its subcontractors have the necessary control over the data processing facilities that are used to process personal data belonging to the controller. This includes any rights of ownership or possession.

(7) The measures in place at the Supplier may be adapted during the course of the Agreement in line with technical and organisational developments. The Supplier shall inform HSBC and its data protection officer without undue delay in documented form (in writing, electronically) of changes to the technical and organisational security measures and of any other changes leading to a reduction in the level of protection.

(8) Any important, security-related decisions concerning the organisation of the data processing and the methods and procedures used must be agreed between the Supplier and HSBC.

§ 11 Permissibility of the establishment of subcontractor arrangements (additional processors) and conditions governing their use

(1) The commissioning of another processor (subcontractor) by the Supplier to perform the service described in the Agreement requires the prior written consent of HSBC. The Supplier must include the name, address, and proposed activity of the subcontractor in its consent request to HSBC. The Supplier must also ensure that it selects the subcontractor carefully, paying special consideration to the suitability of the technical and organisational measures put in place by the subcontractor within the meaning of Art. 32 GDPR. The relevant audit documents are also to be supplied to HSBC.

(2) There shall be no general advance authorisation to the commissioning of subcontractors of the type provided for in Article 28 (2) GDPR. If, by way of exception, such a general consent is explicitly agreed in writing, the Supplier will always inform HSBC of every intended change in respect of the commissioning of additional subcontractors or substitution of existing ones, whereby HSBC shall be given the opportunity to object to such changes. The Supplier will provide meaningful information about the subcontractor to enable HSBC to decide whether to object. If HSBC objects, the subcontractor in question must not be used.

(3) Services commissioned by the Supplier from third parties as ancillary services in support of the commissioned data processing are not subject to the provision in paragraph (1). These include, for example, telecommunications services, maintenance and user services, cleaners, auditors, and the disposal of data storage media. The Supplier is however obliged to enter into legally compliant agreements and to implement control measures to guarantee the protection and the security of HSBC's data even when ancillary services are outsourced.

(4) Subcontractors who were approved as other processors for the performance of the agreed data processing at the time the Agreement was entered into pursuant to paragraph (1) are listed in the '**Approved Subcontractors**' annex. The place of performance and the service commissioned are described for each subcontractor.

(5) The processing of the data by an approved subcontractor is not permitted until the subcontractor has signed an agreement concerning outsourcing pursuant to Article 28 GDPR and has provided evidence to show that appropriate guarantees are in place pursuant to Article 28 (1) GDPR.

(6) The Supplier must ensure that an approved subcontractor is subject to the same contractual obligations as the Supplier itself. In the contract with the subcontractor, the information is to be specified in sufficient detail so that the responsibilities of the Supplier and those of the subcontractor are clearly distinct from one another. If several subcontractors are deployed, this also apples to the division of responsibilities between these subcontractors. In particular HSBC must be entitled, where necessary, to carry out reasonable checks and inspections of the subcontractor, including at the subcontractor's premises, or to have such checks and inspections carried out by a third party instructed by HSBC.

(7) The agreement with the subcontractor must be made in writing or in a documented electronic format.

(8) Data may not be passed on to the subcontractor until the subcontractor has complied with the obligations set forth in § 9 of this annex and Articles 29 and 32 (4) GDPR in respect of its employees.

(9) The Supplier must carry out regular checks to ensure that the subcontractor(s) is/are complying with these obligations. The outcome of the checks must be documented and made available to HSBC upon request.

(10) The processing of personal data by an approved subcontractor is carried out exclusively in the Federal Republic of Germany, in a member state of the European Union, in another of the signatory states to the Treaty on the European Economic Area, or in a third country for which the European Commission has adopted an 'adequacy decision'.

Any processing in other countries or at an international organisation requires the prior written consent of HSBC.

Where consent has been granted, data may be transferred to a third country or to an international organisation only if the special conditions of Chapter V of the GDPR are fulfilled, provided that the Supplier is not required to transfer such data by European Union law or the law of a European Union member state to which it is subject. In such a case, the Supplier shall inform HSBC of these legal requirements prior to processing, so far as the law concerned does not prohibit such notification on the grounds of important public interest.

§ 12 Regular review of the adequacy decision

(1) If data is processed in a third country for which the European Commission has adopted an adequacy decision, as defined in Article 45 GDPR, HSBC and the Supplier will regularly check to ensure that the adequacy decision remains in force[1].

(2) The Supplier will inform HSBC without undue delay as soon as it becomes aware that the adequacy decision is to be or has been reversed, amended, or suspended.

(3) HSBC reserves the right to demand the relocation of the data processing to a member state of the European Union, to another signatory state of the Agreement on the European Economic Area, or to a third country for which the European Commission has adopted an adequacy decision, if the periodic review described in Article 45 (3) sentence 2 in conjunction with Article 45 (5) GDPR indicates that the adequacy decision is to be or has been reversed, amended, or suspended.

§ 13 Other obligations after termination of the Agreement

(1) Documentation that serves as evidence that the data has been processed correctly and lawfully must be retained by the Supplier in accordance with the relevant retention periods after the Agreement has ended. The Supplier may relieve itself of this duty by transferring such documentation to the controller when the Agreement ends. In the event of a recourse claim the Supplier must, even after the Agreement has ended, transfer to the controller any documentation that is still in its possession and is required by the controller to defend itself against any claim for damages relating to alleged unlawful or incorrect data processing.

(2) The Supplier is obliged to maintain confidentiality indefinitely – including after the end of the contractual relationship – in respect of the data and content that became known to it in connection with the commissioned data processing.

§ 14 Liability

[1] See here for list:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

(1) The Supplier shall be liable to pay compensation for any loss or damage suffered by, and to reimburse any additional expenses incurred by, HSBC as the result of data being unlawfully or incorrectly processed by the Supplier on behalf of HSBC in breach of the GDPR or other data protection legislation. Unlawful in this sense includes, but is not limited to, processing that is not in accordance with the provisions of the GDPR or other data protection legislation or the instructions of the controller, and incorrect processing arising from process errors on the part of the Suppler. The Supplier will exempt the controller from any third party claims in this respect.

(2) In other respects, the liability provisions of the aforementioned Agreement apply. If no liability provisions have been agreed in the aforementioned Agreement, the statutory provisions regarding liability apply.

_____
(First name, last name in block letters (HSBC)):

_____ _____
(Place, date) (Signature, HSBC)

_____
(First name, last name in block letters (Supplier)):

_____ _____
(Place, date) (Signature, Supplier)

Annex: 'Data Security'
– Security of processing pursuant to Article 32 GDPR –

Preamble

Taking account of the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, this annex specifies, in accordance with Article 32 GDPR, the technical and organisational measures implemented to ensure a level of security appropriate to the risk arising from the data processing described in detail in the Agreement.

This annex applies to all processing of HSBC's personal data by the Supplier or by subcontractors engaged by the Supplier.

1 Technical and organisational security measures implemented to ensure an appropriate level of data protection

(1a) Measures to **pseudonymise and anonymise** personal data:

Note:
Pseudonymisation is the processing of personal data in such a way that the personal data cannot, without reference to additional information, be used to identify a specific data subject, provided that the additional information is stored separately and is subject to technical and organisational measures that ensure the personal data cannot be associated with an identified or identifiable individual. Anonymisation is where such additional information does not exist or has been irretrievably deleted.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1b) Measures to **encrypt** personal data:

Note:
The encryption of personal data is a commonly used means of protecting such data against access by unauthorised parties.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1c) Measures to **ensure ongoing confidentiality**:

Note:
This refers to measures that guarantee appropriate security of the personal data, including protection against unauthorised or improper processing and against inadvertent loss, destruction, or damage. These measures must be designed so that they guarantee ongoing confidentiality.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1d) Measures to **ensure ongoing integrity**:

Note:
This refers to measures that guarantee appropriate security of the personal data, including protection against unauthorised or improper processing and against inadvertent loss, destruction, or damage as well as unauthorised amendment. These measures must be designed so that they guarantee ongoing integrity.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1e) Measures to **ensure ongoing availability**:

Note:
This refers to measures that protect personal data against accidental destruction or loss. These measures must be designed so that they guarantee ongoing availability.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1f) Measures to **ensure ongoing resilience of the processing systems and services**:

Note:

This includes, for example, measures that are to be implemented by the controller and the supplier prior to commencement of the data processing (cf. 2i). Continuous monitoring of the systems may also be necessary.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1g) Measures to enable the rapid **restoration of availability in the event of a physical or technical incident**:

Note:
Ensuring that personal data can be restored requires adequate backup systems as well as business continuity plans that get systems back up and running after a disaster (using data backups where applicable).
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

(1h) Measures for **regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures**

Note:
Measures that serve in particular to keep the data security measures described here up to date.
Any existing documentation (e.g. in a data protection or security plan) may also be provided.

Annex: Approved Subcontractors

Brief description of activity:	Name of the company:	Registered office, place where the data will be processed:	Data protection officer / person responsible for data protection (First name, last name, contact details):

This notice was last updated on 01 July 2025.