

**Auftrag gemäß Art. 28 DS-GVO
zur Verarbeitung personenbezogener Daten (Auftragsverarbeitung)**

Vereinbarung

zwischen

**Hamburgische Investitions- und Förderbank
Anstalt öffentlichen Rechts
Besenbinderhof 31
20097 Hamburg**

- Verantwortlicher -
- nachstehend Auftraggeber genannt -

und

- Auftragsverarbeiter -
- nachstehend Auftragnehmer genannt -

ggf.: Vertreter gemäß Art. 27 DS-GVO
(von nicht in der Union niedergelassenen Auftragsverarbeitern):

§ 1 Gegenstand und Dauer des Auftrags

- (1) Gegenstand
- (2) Dauer

Der Auftrag beginnt am:

Die Regelung des Dienstleistungsvertrages zur Vertragsdauer/ Kündigung gelten für diese Vereinbarung bzw. in gleicher Weise.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 2 Konkretisierung des Auftragsinhalts

- (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede nachträgliche Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

- (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien):

- ☐ Personenstammdaten (z.B. Name, Anschrift, Geburtsdatum)
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ personenbezogene Daten zu Bank- oder Kreditkartenkonten

- (3) Kreis der Betroffenen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Antragsteller und Empfänger von Corona-Hilfen
- ☐ Kunden
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten/Dienstleister
- ☐ Handelsvertreter
- ☐ Anspruchsteller
- ☐ Ansprechpartner

§ 3 Technisch-organisatorische Maßnahmen (TOM)

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentiert und dem Auftraggeber zur Prüfung übergeben. Die dokumentierten und vom Auftraggeber akzeptierten Maßnahmen werden Grundlage des Auftrags. Soweit eine Prüfung bzw. Audit des Auftraggebers einen Anpassungsbedarf ergibt, so ist dieser einvernehmlich umzusetzen.

- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.
- Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten siehe in den als **Anlage 1** beigefügten technisch-organisatorischen Maßnahmen].
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- (1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt:

Name	Vorname(n)	Tel.-Nr.	E-Mail

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

- (2) Soweit eine gesetzliche Verpflichtung zur Bestellung eines DSB nicht gegeben ist, so ist ein Ansprechpartner für den Datenschutz bekannt zu geben.

Als Datenschutzansprechpartner(in) ist beim Auftragnehmer bestellt:

Name	Vorname(n)	Tel.-Nr.	E-Mail

Ein Wechsel des Datenschutzansprechpartners wird beim Auftraggeber unverzüglich mitgeteilt.

- (3) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- (4) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten siehe in **Anlage 1**].
- (5) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- (6) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- (7) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- (8) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- (9) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnis nach Paragraph 7 dieses Vertrages.
- (10) Wirken Personen des Auftragnehmers und gegebenenfalls von ihm beauftragte Unterauftragnehmer am technischen Vorgang der Erbringung von Telekommunikationsdiensten für den Auftraggeber mit, so erstreckt sich diese Sorgfaltspflicht auch auf das Fernmeldegeheimnis nach § 3 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) 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 mittels unterschriebenen Erklärungsformulars nachzuweisen.
- (11) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

§ 6 Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.
Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Nr.	Firma Unterauftragnehmer	Anschrift / Land	Leistung
1			
2			
3			

4			
5			

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (2 Wochen) vorab (d.h. vor dem Zeitpunkt der vertraglichen Vereinbarung) schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht spätestens 4 Wochen vor dem Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (4) Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung von personenbezogenen Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung auch direkt ggü. den Unterauftragnehmern wahrnehmen kann.
- (5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

§ 9 Weisungsbefugnis des Auftraggebers

Art. 29 DS-GVO sieht vor, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn sie sind nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten zur Verarbeitung verpflichtet.

(1) Weisungsberechtigte Personen beim Auftraggeber sind:

Name	Vorname(n)	Position	Tel.-Nr.	E-Mail

(2) Zur Entgegennahme von Weisungen berechnete Personen beim Auftragnehmer sind:

Name	Vorname(n)	Position	Tel.-Nr.	E-Mail

- (3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechnete, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Haftung

Auf Art. 82 DS-GVO wird verwiesen.

§ 12 Vergütung und Kosten

Die Parteien sind sich einig, dass der Auftragnehmer auch für die Erfüllung der in dieser Vereinbarung geregelten Verpflichtungen durch die in dem Hauptvertrag vorgesehene Vergütung entlohnt wird und dass der Auftragnehmer im Hinblick auf diese Vereinbarung keine darüberhinausgehende Vergütung erhält.

§ 13 Schlussbestimmungen

- (1) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
- (2) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
- (3) Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Fall, dass der Auftraggeber ein Kreditinstitut ist oder personenbezogene Daten eines Kreditinstituts der Unternehmensgruppe des Auftraggebers verarbeitet werden, wird zusätzlich die nachstehende Regelung vereinbart:

Da der Auftraggeber dem Bankgeheimnis¹ unterliegt, gelten die Verpflichtungen für die Wahrung des Bankgeheimnisses auch für den Auftragnehmer und gegebenenfalls für von ihm beauftragte Unterauftragnehmer. Die vom Auftragnehmer eingesetzten Mitarbeiter und gegebenenfalls von ihm beauftragten Unterauftragnehmer sind zur absoluten Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet. Informationen über den Kunden dürfen nur vom Auftraggeber selbst oder vom Auftragnehmer nach vorheriger schriftlicher Zustimmung des Auftraggebers weitergegeben werden, wenn gesetzliche Bestimmungen dies gebieten oder der Kunde eingewilligt hat oder der Auftraggeber zur Erteilung einer Bankauskunft befugt ist.

¹ Das Kreditinstitut ist zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet, von denen sie Kenntnis erlangt (Bankgeheimnis). Informationen über den Kunden darf das Kreditinstitut nur weitergeben, wenn gesetzliche Bestimmungen dies gebieten oder der Kunde eingewilligt hat oder das Kreditinstitut zur Erteilung einer Bankauskunft befugt ist. Abweichend kann das Recht eines Mitgliedsstaats der Europäischen Union ein Bankgeheimnis vorsehen.

.....
(Datum, Ort)

.....
(Datum, Ort)

.....
(Unterschrift Auftraggeber)

.....
(Unterschrift Auftraggeber)

.....
(Name des Unterzeichners im Klartext)

.....
(Name des Unterzeichners im Klartext)

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers