

Auftragsverarbeitungsvertrag (AVV)

zwischen

Investitions- und Förderbank Niedersachsen - NBank
Günther-Wagner-Allee 12-16
30177 Hannover
(kurz: „Auftraggeber“)

und

Name
Anschrift
(kurz: „Auftragnehmer“)

Präambel

Der vorliegende Auftragsverarbeitungsvertrag (kurz: „AVV“) konkretisiert für alle Verarbeitungen die Rechte und Pflichten der Parteien auf dem Gebiet des Datenschutzes, welche sich aus den zwischen den Parteien bereits oder künftig bestehenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen (kurz: „Hauptvertrag“) ergeben.

§ 1 Auftrag und Spezifika der Verarbeitung

- (1) Der AVV kommt mit all seinen Teilen zur Anwendung, sofern und soweit der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (kurz: „**Daten**“) verpflichtet hat.
- (2) Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.
- (3) Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV und all seiner Teile den Regelungen des zugehörigen Hauptvertrages vor.
- (4) Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „**Spezifika**“) werden vor Beginn der Verarbeitung in der Anlage zum AVV (kurz: „**A-AVV**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (kurz: „**TOM**“).
- (5) Die A-AVV ist Teil des AVV. Bei etwaigen Widersprüchen gehen die Regelungen der A-AVV der allgemeineren Regelung im AVV vor. Wird im

Folgenden oder in den A-AVV auf den AVV Bezug genommen, so ist der AVV mit allen seinen Teilen gemeint.

- (6) Werden in der AVV und A-AVV die in der Datenschutz Grundverordnung (VO (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725) definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in den betreffenden Verordnungen. Die Bestimmungen sind im Lichte der Verordnungen auszulegen.

§ 2 Verantwortlichkeit und Verarbeitung auf Weisung

- (1) Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).
- (2) Der Auftragnehmer verarbeitet die personenbezogenen Daten nur für den/die in A - AVV genannten spezifischen Zweck(e) für die dort angegebene Dauer, sofern er keine weiteren Weisungen des Auftraggebers erhält. Der Auftragnehmer handelt ausschließlich weisungsgebunden, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
- (3) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „**Sperrung**“), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Nach Beendigung des Auftrags ist der Auftragsverarbeiter verpflichtet die erhaltenen Daten vollständig zu löschen und hierüber einen Nachweis gegenüber dem Verantwortlichen zu erbringen.
- (4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.
- (5) Die Parteien benennen in Textform gegenseitig einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

- (6) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.
- (7) Der Auftragnehmer gewährt eingesetztem Personal Zugang zu den personenbezogenen Daten, die Gegenstand dieser Vereinbarung sind, nur insoweit als dies für die Durchführung, Verwaltung und Überwachung des Vertrages unbedingt erforderlich ist. Ferner wird durch den Auftragnehmer sichergestellt, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.
- (8) Der Auftragnehmer hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren, soweit der Auftraggeber dem Bankgeheimnis unterworfen ist. Hierauf wird der Auftraggeber den Auftragnehmer hinweisen, sofern dies für den Auftragnehmer aus dem Hauptvertrag nicht ersichtlich ist. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die dem Auftraggeber über seine Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob der Auftraggeber überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

§ 3 Sicherheit der Verarbeitung

- (1) Die Parteien vereinbaren technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten, um diese vor einer Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von Daten führt, zu schützen.
- (2) Falls die Verarbeitung personenbezogener Daten im Sinne des Art. 9 oder Art. 10 DSGVO betrifft, wendet der Auftragnehmer spezielle Beschränkungen und/oder zusätzlichen Garantien an.
- (3) Änderungen der vereinbarten TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.
- (4) Trifft der Auftraggeber eigene technische und organisatorische Maßnahmen für eine auf den Auftragnehmer übertragene Datenverarbeitung, so hat ihn der Auftragnehmer im Rahmen seiner Möglichkeiten hierbei zu unterstützen.

§ 4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

- (1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber offengelegten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht.
- (2) Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu unterrichten.
- (3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 4 (1) oder der Fehler gemäß § 4 (2) sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen gemäß § 4 (1) oder § (2) sind unverzüglich in Textform nachzureichen.
- (4) Die Meldung nach § 4 (1) enthält alle Informationen, die gemäß Artikel 33 Absatz 3 der DS-GVO oder Artikel 34 Absatz 3 der DS-GVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen:
 - a) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
 - b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
 - c) die voraussichtlichen Folgen und die ergriffenen oder vorgesehenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

§ 5 Übermittlung von Daten an einen Empfänger in einem Drittland

Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B.

Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Dies gilt auch, wenn der Auftragsnehmer einen Unterauftragsverarbeiter gemäß § 6 AVV für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt.

§ 6 Unterbeauftragung weiterer Auftragsverarbeiter

- (1) Der Auftragsnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „**Unterauftragsnehmer**“) erbringen lassen.
- (2) Der Auftragsnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragsnehmern oder Änderungen in der Unterbeauftragung und stellt die für die Beurteilung der Unterbeauftragung notwendigen Informationen bereit. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragsnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.
- (3) Der Auftragsnehmer wird mit dem Unterauftragsnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragsnehmer zu vereinbarenden TOM mindestens dasselbe Schutzniveau aufweisen. Der Auftragsnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsnehmer den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- (4) Der Auftragsnehmer vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Auftraggeber– im Falle, dass der Auftragsnehmer faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.
- (5) Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragsnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragsnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der

Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§ 7 Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

§ 8 Kontroll- und Informationsrechte des Auftraggebers

- (1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.
- (2) Für die Überprüfung der Einhaltung der vereinbarten Schutzmaßnahmen nach § 3 (1) und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach SITB (Sicherer IT-Betrieb der Sparkassen-Finanzgruppe), eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Des Weiteren können andere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 8 (3) bleibt hiervon unberührt.
- (3) Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Der Auftraggeber kann die

Prüfung selbst durchführen oder einen unabhängigen Prüfer mit der Prüfung beauftragen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

- (4) Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.
- (5) Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich, bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

§ 9 Haftung und Schadenersatz

- (1) Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.
- (2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.
- (3) Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.
- (4) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

§ 10 Laufzeit

- (1) Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer A-AVV wird in der A-AVV selbst geregelt; ohne eine solche Regelung entspricht die Laufzeit einer A-AVV derjenigen des AVV.
- (2) Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle A-AVV beendet wurden.
- (3) Eine A-AVV endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser A-AVV bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der A-AVV verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform (z. B. durch ein Löschprotokoll) zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur

Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

- (4) Der Auftraggeber ist berechtigt, den Hauptvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung betrifft, wenn
- a) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß § 12 Absatz 2 ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - b) der Auftragsnehmer in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DS-GVO nicht erfüllt;
 - c) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- (5) Der Auftragsnehmer ist berechtigt, den Hauptvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragnehmer darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen (§ 2 Absatz 4) verstoßen.

§ 11 Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab dem 25.05.2018 die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Spezifika vereinbart, so gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch A-AVV ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

§ 12 Schlussbestimmungen

- (1) Sollten die Daten des Auftraggebers 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 in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.
- (2) Falls der Auftragsnehmer seinen Pflichten gemäß des AVV und der A-AVV nicht nachkommt, kann der Auftraggeber den Auftragsnehmer anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er die AVV und die AAVV einhält oder der Vertrag beendet ist. Der Auftragnehmer unterrichtet den

Auftraggeber unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Vereinbarungen einzuhalten.

- (3) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.
- (4) Sollte auch nur eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.
- (5) Es gilt deutsches Recht.

Ort, Datum

Ort, Datum

Unterschrift

Unterschrift

Name, Fachbereich NBank

Name, Funktion Unterzeichner
(in Druckbuchstaben)