

## **Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO**

The new freedom in business communications.

[nfon.com](https://nfon.com)

<b>1</b>	<b>GEGENSTAND UND DAUER DES AUFTRAGS</b>	<b>5</b>
<b>2</b>	<b>KONKRETISIERUNG DES AUFTRAGSINHALTS</b>	<b>5</b>
<b>3</b>	<b>TECHNISCH-ORGANISATORISCHE MAßNAHMEN</b>	<b>6</b>
<b>4</b>	<b>BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN</b>	<b>7</b>
<b>5</b>	<b>QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS</b>	<b>7</b>
<b>6</b>	<b>UNTERAUFTRAGSVERHÄLTNISSE</b>	<b>8</b>
<b>7</b>	<b>KONTROLLRECHTE DES AUFTRAGGEBERS</b>	<b>9</b>
<b>8</b>	<b>MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS</b>	<b>10</b>
<b>9</b>	<b>WEISUNGSBEFUGNIS DES AUFTRAGGEBERS</b>	<b>10</b>
<b>10</b>	<b>LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN</b>	<b>10</b>
<b>11</b>	<b>UNTERSCHRIFTEN</b>	<b>12</b>

**Version 1.4**

NFON AG  
Zielstattstraße 36,  
81379 München  
Tel.: + 49 89 45 3000  
[www.nfon.com](http://www.nfon.com)

© 2024 NFON AG – Alle Rechte vorbehalten

Änderungen bleiben vorbehalten  
Version 1.4/ 01.2024 (DE)  
gültig ab dem 01.01.2024

**Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO**

zwischen dem / der

- nachstehend Auftraggeber genannt –  
und der

NFON AG, Zielstattstraße 36, 81379 München

- nachstehend Auftragnehmer genannt -



*„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“*

## 1 Gegenstand und Dauer des Auftrags

### 1.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Angebot, der aktuell gültigen Leistungsvereinbarung und den jeweils gültigen AGB.

### 1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

## 2 Konkretisierung des Auftragsinhalts

### 2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der vereinbarten Leistungsvereinbarung.

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

### 2.2 Art der Daten

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

- Personenstammdaten
- Vertragsstammdaten/ Kontodaten
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Verbindungsdaten (IP-Adresse, A- und B-Rufnummer, Gesprächsdauer)
- Gesprächsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

## 2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Kommunikationspartner

## 3 Technisch-organisatorische Maßnahmen

- 3.1** 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 zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3.2** 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 in Anlage 1].
- 3.3** 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.
- 3.4** Werden die technischen und organisatorischen Maßnahmen geändert und/oder ergänzt, veröffentlicht der Auftragnehmer diese angemessen. Eine angemessene Information über die üblichen Kommunikationswege besteht aus der Veröffentlichung eines Konzeptes, welches der Auftraggeber mit verhältnismäßigem Aufwand einsehen kann. Der Auftragnehmer legt fest, auf welchen Wege die Informationen bereitgestellt werden. Nach Bekanntgabe wird dem Auftraggeber eine Frist zum Widerspruch eingeräumt. Die Frist beträgt zwei Wochen. Ist diese Frist abgelaufen, gelten die technischen und organisatorischen Maßnahmen seitens des

Auftraggebers als genehmigt. Einsprüche müssen schriftlich formlos an datenschutz@nfon.com gemeldet werden.

## 4 Berichtigung, Einschränkung und Löschung von Daten

- 4.1** 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 keine gesetzlichen Anforderungen dazu verpflichten. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- 4.2** 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 Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich verpflichtend, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
- Die Kontaktdaten des Datenschutzbeauftragten werden auf der Homepage des Auftragnehmers veröffentlicht.
- Die Wahrung der Vertraulichkeit gemäß Artt. 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese konkrete und grundsätzliche Beauftragung beziehen und dies gesetzlich nicht verboten. 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.
- 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, soweit dies gesetzlich erlaubt ist.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6 Unterauftragsverhältnisse

- 6.1** 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, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie 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.
- 6.2** Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen, soweit er den Auftraggeber angemessen vorab deren Beauftragung informiert. Eine angemessene Information besteht aus der Veröffentlichung der bestehenden und neuer Unterauftragnehmer, die der Auftraggeber mit verhältnismäßigem Aufwand einsehen kann. Die Informationen werden über die üblichen Kommunikationskanäle bereitgestellt. Nach Bekanntgabe wird dem Auftraggeber eine Frist zum Widerspruch eingeräumt. Die Frist beträgt zwei Wochen. Ist diese



Frist abgelaufen, gilt der Unterauftragnehmer seitens des Auftraggebers als genehmigt. Einsprüche müssen schriftlich formlos an [datenschutz@nfon.com](mailto:datenschutz@nfon.com) gemeldet werden.

- 6.3** Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Solche Maßnahmen müssen auch für Dienstleistungsanbieter durchgeführt werden, die Nebenleistungen erbringen.
- 6.4** Sämtliche vertraglichen Regelungen in der Vertragskette sind auch weiteren Unterauftragnehmern aufzuerlegen. Die technischen und organisatorischen Maßnahmen von Unterauftragnehmern sind an die hier definierten technischen und organisatorischen Maßnahmen angelehnt, können aber ein risikoorientiertes geringeres Niveau besitzen.

## 7 Kontrollrechte des Auftraggebers

- 7.1** 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 und spätestens 14 Tage vorab anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- 7.2** 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.
- 7.3** 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, Qualitäts-auditoren);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO27001).

## 8 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 9 Weisungsbefugnis des Auftraggebers

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

## 10 Löschung und Rückgabe von personenbezogenen Daten

- 10.1** 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.
- 10.2** 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.

- 10.3** 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 Unterschriften

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Name des Auftraggebers

\_\_\_\_\_  
Name des Auftragnehmers

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Name des Auftraggebers

\_\_\_\_\_  
Name des Auftragnehmers