

BESTIMMUNGEN ZUM DATENSCHUTZ ANLÄSSLICH DER TEILNAHME AM CLEARING-CENTER DER NTG

I. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach der Teilnahmevereinbarung zum Clearing-Center der NTG (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

II. Umfang der Beauftragung

- a. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.
- b. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **ANLAGE 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.
- c. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

III. Weisungsbefugnisse des Auftraggebers

- a. Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- b. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers.
- c. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

IV. Verantwortlichkeit des Auftraggebers

- a. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.
- b. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

V. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

VI. Sicherheit der Verarbeitung

- a. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.
- b. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen (TOM) während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen. Die derzeitigen TOM ergeben sich aus der **ANLAGE 2**.

VII. Inanspruchnahme weiterer Auftragsverarbeiter

- a. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus **ANLAGE 1**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.
- b. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

- c. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.
- d. Unter Einhaltung der Anforderungen dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

VIII. Rechte der betroffenen Personen

- a. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
- b. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
- c. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
- d. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.
- e. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

IX. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

- a. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen.

- b. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

X. Datenlöschung

- a. Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.
- b. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

XI. Nachweise und Überprüfungen

- a. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
- b. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.
- c. Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 17 Uhr) nach rechtzeitiger Vorankündigung auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.
- d. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.
- e. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.
- f. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder

Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z. B. nach BSI-Grundschrift – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

XII. Vertragsdauer und Kündigung

Die Laufzeit und die Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags.

XIII. Haftung

Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

XIV. Schlussbestimmungen

- a. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.
- b. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

ANLAGE 1

Zweck der Datenverarbeitung: Leistungen des Clearing-Centers der NTG, DI-Datenaustausch, Nachrichtenaustausch

Datenkategorie: Kommunikationsdaten (Telefon, E-Mail), Vertragsdaten, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten (z. B. Sales Reports und Inventory Reports)

Kreis der Betroffenen: Kunden/Vertragspartner, Mitarbeiter

ANLAGE 2

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Im Folgenden werden die technisch-organisatorischen Maßnahmen aufgeführt, die für folgendes Unternehmen gelten:

NTG connect GmbH

Series-A Campus, Sophienstraße 1, 51149 Köln

INHALT

1. Pseudonymisierung
2. Verschlüsselung
3. Gewährleistung der Vertraulichkeit
4. Gewährleistung der Integrität
5. Gewährleistung der Verfügbarkeit

6. Gewährleistung der Belastbarkeit der Systeme
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen und technischen Zwischenfall
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

1. Pseudonymisierung

Keine Maßnahmen

2. Verschlüsselung

- Sicherung bei der elektronischen Übertragung
- Zertifikatsbasierte Zugangsberechtigung (VPN)
- Verschlüsselung von Datenträgern

3. Gewährleistung der Vertraulichkeit

- Elektronische Türschlösser mit individuell programmierbaren Schlüsseln
- Videoüberwachter Eingangsbereich
- Videoüberwachung (wenn Alarm eingeschaltet ist)
- Alarmanlagen
- Dauerhaft besetzter Empfang
- Firewall
- Zertifikatsbasierte Zugangsberechtigung (VPN)
- gesicherte Schnittstellen (Netzwerk)
- Aktenvernichter
- Berechtigungskonzept
- Verschlüsselung von Datenträgern
- Sicherung bei der elektronischen Übertragung
- Löschkonzept

4. Gewährleistung der Integrität

- Zugang zu Rechnern/Systemen (Authentifizierung)
- Benutzererkennung mit Passwort
- Passwortvergabe / Passwortregeln
- Firewall
- gesicherte Schnittstellen (Netzwerk)
- Berechtigungskonzept
- Verschlüsselung von Datenträgern
- Sicherung bei der elektronischen Übertragung
- Fax-Protokoll
- Protokollierung (Serverlogs)
- Benutzeridentifikation
- Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsverarbeitung)
- separate Tabellen innerhalb von Datenbanken
- getrennte Datenbanken

5. Gewährleistung der Verfügbarkeit

- Brandschutzmaßnahmen
- Überspannungsschutz
- Unterbrechungsfreie Stromversorgung
- Klimaanlage
- RAID (Festplattenspiegelung)
- Backupkonzept
- Virenschutzkonzept

6. Gewährleistung der Belastbarkeit der Systeme

- Skalierbare Systeme
- Rechenzentrum
- Virtualisierung

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten

nach einem physischen oder technischen Zwischenfall

- RAID (Festplattenspiegelung)
- Virtualisierung
- Redundante Systeme
- Backupkonzept

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der

Wirksamkeit der technischen und organisatorischen Maßnahmen

Jährliches internes Audit der technischen und organisatorischen Maßnahmen durch den

externen Datenschutzbeauftragten iSd EU-Datenschutzgrundverordnung.

CONTRACT DATA PROCESSING OF ORDERS

I. Subject matter of the contract

Within the framework of service provision according to the participation agreement at the Clearing-Center of NTG (hereinafter referred to as “**main contract**”), it is necessary that the contractor uses personal data for which the principal acts as responsible body in accordance with the current data protection regulations (hereinafter referred to as “**the principal’s data**”). This contract substantiates the data protection rights and obligations of the parties in connection with the contractor’s handling of the principal’s data for the implementation of the main contract.

II. Extent of the Commissioning

- a. The contractor processes the principal’s data on behalf of and according to instruction of the principal in accordance with Art. 28 DSGVO (order processing). The principal remains responsible in the sense of the data protection regulations.
- b. The processing of the principal’s data by the contractor is effected as specified in **ENCLOSURE 1** to this contract as far as type, extent and purpose are concerned; the processing concerns the types of personal data and categories of persons affected.
- c. The processing of the principal’s data by the contractor basically takes place within the European Union or in another contractual state of the Agreement on the European Economic Area (EEA). Nevertheless, the contractor is allowed to also process the principal’s data under observation of the contractual regulations in non-EEA countries if he has informed the principal on the place of data processing beforehand and the prescriptions of article 44 - 48 DSGVO are fulfilled or if there is an exception due to article 49 DSGVO.

III. Authority of the principal

- a. The contractor processes the principal’s data according to the instructions of the principal provided that the contractor is not obliged to other processings. In the latter case, the contractor informs the principal on these legal requirements before the processings if the law concerned does not prohibit such an information because of an important public interest.
- b. The instructions of the principal are fundamentally determined, recorded and concluded in the regulations of this contract. Individual instructions which deviate from the determinations in this contract or place additional requirements require the prior consent by the contractor.
- c. The contractor guarantees that he processes the principal’s data in accordance with the instructions of the principal. If the contractor is of the opinion that an instruction from the principal violates this contract or the current data protection law, he is entitled to suspend the principal’s instruction after prior information until the principal confirms the instruction. The parties agree that the sole responsibility for processing the principal’s data as directed lies with the principal.

IV. Responsibilities of the principal

- a. The principal is solely responsible for the legality of the processing of the principal’s data as well as the protection of the rights of the affected within the relationship of the parties to each other. If claims from third parties will arise due to the processing of the principal’s data according to this contract, the principal will indemnify the contractor from all such claims on first demand.

- b. If the contractor is obliged to inform a governmental authority or person on the processing of the principal’s data or to cooperate with such authorities in other matters, the principal is obliged to support the contractor on first demand with the provision of such information and/or the fulfillment of other obligations of cooperation.

V. Employee requirements

The contractor must oblige all personnel processing the principal’s data to confidentiality concerning the processing of the principal’s data.

VI. Security of processing

- a. The contractor will, according to article 32 DSGVO, take necessary and appropriate technical and organizational measures which will guarantee a protection level appropriate to the risks for the principal’s data, under consideration of the technical state-of-the-art, the implementation costs and the type, the extent, the circumstances and the purposes of the processing of the principal’s data as well as the different probabilities of occurrence and severity of the risks concerning the rights and liberties of the persons concerned.
- b. The contractor is allowed to modify or change technical and organizational measures (TOM) during the contract period as long as they still meet the legal provisions. The current TOM measures are stated in **ENCLOSURE 2**.

VII. Utilisation of further order data processors

- a. Herewith, the principal grants the contractor the general permission to add further order data processors for the processing of the principal’s data. The further order data processors added at the period of the contract implementation can be seen on **ENCLOSURE 1**. Contractual relationships with service providers who provide verifications or maintenance of data processing operations or data processing systems by other bodies or other auxiliary services are not subject to authorization as long as the contractor implements appropriate regulations to protect the confidentiality of the principal’s data.
- b. The contractor will inform the principal on intended modifications in relation to the additional involvement or replacement of further order data processors. In the individual case, the principal is entitled to the right to raise an objection against the assignment of a potential further order data processor. An objection may only be raised for good cause which has to be proven to the contractor. If the principal does not raise an objection within 14 days after receipt of the information, his right to raise an objection concerning the respective involvement shall become null and void. If the principal raises an objection, the contractor is entitled to terminate the main contract and this contract within a period of 3 months.
- c. The contract between the contractor and the further order data processor must oblige the latter to the same obligations as is the contractor given under this contract. The parties agree that this requirement is fulfilled if the contract exhibits a protection level appropriate to this contract and / or the further order data processor is imposed to the obligations mentioned in article 28 section 3 DSGVO.
- d. Besides the compliance to the requirements of this contract, the regulations of this clause 7 also apply when a further order data processor in a third country is involved. The principal herewith authorizes the contractor to conclude, in the name and on behalf of the principal, a contract with a further order data processor under inclusion of the EU standard contract clauses for the transmission of personal data to order data processors in third countries of 5th February 2010. The principal agrees to contribute to the fulfillment of the

prerequisites according to article 49 DSGVO to the necessary extent.

VIII. Rights of the persons concerned

- a. The contractor will support the principal with technical and organizational measures within reasonable bounds to meet his obligation of answering applications on fulfilling the rights of persons concerned.
- b. If a person concerned directly asserts an application on meeting their legal rights towards the contractor, the contractor will pass this application to the principal in due time.
- c. The contractor will communicate details on the principal's data saved, the recipients of the principal's data who obtain the principal's data as ordered and the reason for saving the data if the principal does not have this details available or he can obtain them himself.
- d. The contractor will enable the principal to correct, to delete or limit the further processing of the principal's data to a reasonable extent and if necessary or will, on the principal's request, effect the correction, blocking or restriction of the further processing himself, if the principal cannot do so himself.
- e. If the person concerned is entitled towards the principal to transmit data concerning the principal's data according to article 20 DSGVO, the contractor will, within the framework of the tolerable and necessary, support the principal against reimbursement of costs and efforts arising at the provision of the principal's data in a conventional and machine-readable format if the principal cannot obtain the data otherwise.

IX. Information and support obligations of the contractor

- a. If the principal is affected by a legal report and notification obligation because of a violation of the protection of the principal's data (especially according to article 33, 34 DSGVO), the contractor will inform the principal on possible report obligations on events in his area of responsibility in due time. The contractor will support the principal in fulfilling the report and notification obligations on his request within the framework of the tolerable and necessary.
- b. The contractor will support the principal within the framework of the tolerable and necessary with data protection impact assessments and possible resulting consultations by the supervisory authorities according to article 35, 36 DSGVO.

X. Data deletion

- a. The contractor will delete the principal's data after expiration of this contract if the contractor has no legal obligation to the continued storing of the principal's data.
- b. After expiration of the contract, the contractor may store documentations which serve as evidence of proper processing of the principal's data as ordered.

XI. Evidence and verifications

- a. The contractor will provide the principal on his request with all necessary information and all information which is available to the contractor to prove the observation of his obligations according to this contract.
- b. The principal is entitled to monitor the contractor (including inspections) concerning the observation of the regulations of this contract, especially the implementation of the technical and organizational measures.
- c. Concerning the execution of inspections according to clause 11.2, the principal is entitled to enter the premises of the contractor where the principals data are processed during normal business hours (Monday to Friday from 10 until 17 h)

with prior notice at his own expenses, without disturbing the working process and under strict confidentiality of trade and company secrets of the contractor.

- d. The contractor is entitled, at his own discretion and under consideration of the legal obligations of the principal, not to disclose data which are sensitive with regard to the transactions of the contractor or if the contractor would violate legal or other contractual regulations by their disclosure. The principal is not entitled to gain access to data or details on other customers of the contractor, details on costs, on quality verification and contractual management reports as well as all other confidential data of the contractor which are not of direct relevance for the agreed validation purposes.
- e. If the principal instructs a third party with the execution of the verification, the principal must oblige the third party to the same obligations as is the principal towards the contractor according to this clause 11 of this contract. Furthermore, the principal must oblige the third party to discretion and confidentiality unless the third party is subject to a professional confidentiality obligation. The principal must present the obligation agreements with the third party immediately upon request of the contractor. The principal is not allowed to commission a competitor of the contractor with the inspection.
- f. According to the choice of the contractor, the evidence of the observation of the obligations in this contract can, instead of an inspection, also be provided in the form of an appropriate, current certification or report by an independent authority (i.e. auditor, audit, data protection officer, IT security department, data protection auditors or quality auditors) or an appropriate certification by an IT security or data protection audit – e.g. according to BSI basic protection – (“inspection report”), if the inspection report enables the principal to appropriately convince himself of the observation of the contractual obligations.

XII. Contract period and termination

The contract period and the termination of this contract are governed by the regulations concerning the contract period and the termination of the contract. The termination of the main contract will also cause a termination of this contract.

XIII. Liability

The exclusions and limitations of liability according to the main contract will also apply for the principal's liability in this contract. If third parties make any claims towards the contractor which are caused by a culpable infringement by the principal of this contract or one of his obligations as the responsible body for data protection, the principal shall indemnify the contractor against these claims on first request.

XIV. Final Provisions

- a. If individual regulations of this contract become ineffective or if there are any gaps in this contract, the other regulations shall remain untouched. The parties agree to replace the ineffective regulation with a legally permitted regulation which closest approximates the purpose of the ineffective regulation and meets the requirements of article 28 DSGVO.
- b. In case of contradictions between this contract and other agreements between the parties, especially the main contract, the regulations of this contract shall take precedence.

ENCLOSURE 1

Purpose of the data processing: Services of the NTG Clearing Center, EDI data exchange, message exchange

Category of Data: Communication data (telephone, e-mail), contract data, contract billing and payment data, planning and control data (e.g. sales reports and inventory reports)

Parties Affected: Customers/ contractual partners, employees

ENCLOSURE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

According to article 32 section 1 DSGVO for people responsible (article 30 section 1 part g) and data processors (article 30 section 2 part d)

In the following are presented the technical and organizational measures valid for the following company:

NTG connect GmbH

Series-A Campus, Sophienstraße 1, 51149 Köln

CONTENTS

1. Pseudonymization
2. Encoding
3. Safeguarding of the Confidentiality
4. Safeguarding of the Integrity
5. Safeguarding of the Availability
6. Safeguarding of the System Resilience
7. Recovery procedures for the availability of personal data after a physical and technical incident
8. Procedure of regular verification, rating and evaluation of the effectiveness of the technical and organizational measures

1. Pseudonymization

No measures

2. Encoding

- Electronic transmission backup
- Certificate-based access authorization (VPN)
- Data media encoding

3. Safeguarding of the confidentiality

- Electronic door locks with individually programmable keys
- Video-monitored entrance
- Video monitoring (when the alarm is switched on)
- Alarm systems
- Permanently occupied reception area
- Firewall
- Certificate-based access authorization (VPN)
- Secured interfaces (network)
- Document shredders
- Authorization concept
- Encoding of data media

- Electronic transmission protection
- Deletion concept

4. Safeguarding of the integrity

- Access to computers/systems (authentication)
- User ID with password
- Password assignment/ password rules
- Firewall
- Secured interfaces (network)
- Authorization concept
- Encoding of data media
- Electronical data transmission protection
- Fax protocol
- Logging (server logs)
- User identification
- Separation of productive and test systems
- Separated file structures (order processing)
- Separate charts within data bases
- Separate data bases

5. Safeguarding of the availability

- Fire protection measures
- Overvoltage protection
- Uninterruptible power supply
- Air conditioning
- RAID (hard disk mirroring)
- Backup concept
- Anti-virus protection concept

6. Safeguarding of the system resilience

- Scalable systems
- Computer center
- Virtualization

7. Recovery procedures for the availability of personal data after a physical and technical incident

- RAID (hard disk mirroring)
- Virtualization
- Redundant systems
- Backup concept

8. Procedure of regular verification, rating and evaluation of the effectiveness of the technical and organizational measures

Yearly internal audit on the technical and organizational measures by the data protection officer according to the iSd EU data protection regulation.