hogrefe

# Datenschutz bei Hogrefe

Verantwortungsvoller Umgang mit sensiblen Daten

Version: 1.13

Hogrefe Verlag

Merkelstraße 3
37085 Göttingen
Germany

Tel. +49 551 999 50 0
Fax +49 551 999 50 111
info@hogrefe.de
www.hogrefe.de

# Inhalt

# I. Kontaktinformation

Hogrefe Verlag GmbH & Co. KG
Testzentrale
Herbert-Quandt-Str. 4
D-37081 Göttingen
Tel: +49 (0)551 999 50-880
FAX: +49 (0)551 999 50-998
E-Mail: e-tests@testzentrale.de
Internet: www.testzentrale.de

Bei Fragen rund um den Hogrefe Datenschutz wenden Sie sich bitte an:

**Felix Hudy & Laura L. Stoll**
Externe betrieblicher Datenschutzbeauftragte bei Hogrefe
Merkelstraße 3
D-37085 Göttingen
E-Mail: datenschutz@hogrefe.de

# II. Allgemeine Hinweise zum Hogrefe-Datenschutz

## 1. Erläuterung zum Datenschutz im Hogrefe Testsystem (Online-Portal)

Der Datenschutz umfasst drei übergeordnete Aspekte, deren Einhaltung und Umsetzung für einen zuverlässigen Umgang mit dem Hogrefe Testsystem (HTS) unablässig sind:

a. Schutz personenbezogener Daten vor Missbrauch
b. Schutz elektronischer Daten gegen Verlust oder Veränderung
c. Testschutz als Schutz von Tests und Prinzipien der Auswertung gegen ein allgemeines Bekanntwerden

## 2. Allgemein

Das Prinzip „Der beste Datenschutz ist die Vermeidung schutzwürdiger Daten“ kann mit dem HTS umgesetzt werden. Es ist grundsätzlich nicht notwendig, schutzrelevante personenbezogene Daten im HTS zu erfassen. Lediglich das Alter in Jahren und Geschlecht sind für die Anwendung der zutreffenden Normen bei einigen Tests notwendig – die aber für sich genommen keine Identifikation einer Person ermöglichen. Die Identifikation der Person für den Diagnostiker kann über einen individuellen Code (z.B. eine Nummer in einer eigenen Probandenverwaltung) eingegeben werden. Die Dokumentation der Zuordnung „Ergebnis zu Person“ kann außerhalb des HTS erfolgen.

Für die generelle Verwendung von Personendaten im diagnostischen Prozess (Eingabe von Namen, Geburtsdaten, Adressdaten, u.a. während der Testung) trägt daher der Diagnostiker die Verantwortung und muss die Einwilligung für die Verarbeitung personenbezogener Daten einholen, bzw. den für ihn geltenden rechtlichen Rahmen berücksichtigen.

Den datenschutzrechtlichen Löschverpflichtungen kann in HTS vollumfänglich entsprochen werden. Daten auf den Servern werden jedoch nicht automatisch gelöscht. Dies muss der Diagnostiker selbst tun bzw. aktivieren. Unter der Rubrik „Auswerten“ gibt es eine Lösch-Option für Personen; hierbei werden **alle** Messungen der gegebenen Person ebenfalls gelöscht. Im Supervisor-Login lässt sich außerdem eine automatische Löschfunktion für Personen und Testergebnisse aktivieren.

Die Daten werden automatisch in einem Backup-System archiviert, um sie bei Havarien wiederherstellen zu können. Um der gesetzlichen Nachweispflicht nachkommen zu können, empfehlen wir dennoch, den Ergebnisausdruck auf Papier oder elektronisch selbst zu archivieren.

# 3. Schutz personenbezogener Daten vor Missbrauch

Es wird besonderer Wert auf die vertrauliche Behandlung persönlicher Daten und die Einhaltung geltender Datenschutzbestimmungen gelegt. Personenbezogene Informationen, die im Hogrefe Testsystem gespeichert werden, werden nur im Rahmen der hier aufgeführten Richtlinien verarbeitet.

Die Verbindungen zwischen Client (Online-Portal Administrationsplatz) und Server (hogrefe-online.com) auf der einen, sowie Client (Testplatz) und Server (hogrefe-online.com) auf der anderen Seite, erfolgen ausschließlich über verschlüsselte SSL-Verbindungen.

Um die Exaktheit und Sicherheit persönlicher Daten sicherzustellen und um unerlaubten Zugriff oder unsachgemäße Benutzung zu verhindern, werden aktuelle Sicherungsverfahren eingesetzt. Dazu zählen:

- Verwendung von Form-based Authentification
- Datentransfer durch eine TLS-verschlüsselte Verbindung
- Absicherung der Server durch Firewall-Systeme
- Zugriff auf die Server ist auf Port 443 beschränkt

Der Administrationsplatz (Online-Portal) wird durch eine eigene Benutzerverwaltung gesichert, welche sicherstellt, dass nur die vom Benutzer verwalteten Daten auch diesem Benutzer einsehbar sind. Der Hogrefe-Support kann keine Personendaten einsehen, ohne dass der Kunde dem zustimmt.

# 4. EU-Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)

Das HTS erfüllt die datenschutzrechtlichen Anforderungen der DSGVO und des BDSG. Es wird schon bei der Entwicklung besonderer Wert auf Datenschutzfreundlichkeit der Produktgestaltung und auf datenschutzfreundliche Voreinstellungen gelegt, um den Grundsätzen von „privacy by design“ und „privacy by default“ (Art. 25 DSGVO) gerecht zu werden. Im Ergebnis ist eine Verwendung von HTS gänzlich ohne die Erfassung personenbezogener Daten möglich.

Sämtliche mit HTS zusammenhängenden Verarbeitungstätigkeiten und internen Prozesse sind dokumentiert und werden regelmäßig überprüft. Um den Diagnostiker bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen zu unterstützen ist unter VI. die Übersicht der Verarbeitungstätigkeit gem. Artikel 30 Abs. 2 DSGVO dargestellt.

Alle Mitarbeiter werden regelmäßig zu den Anforderungen der DSGVO geschult und sind auf die Vertraulichkeit verpflichtet.

# 5. Sicherheit der Verarbeitung

Um die Sicherheit der Verarbeitung zu gewährleisten, wurden für HTS angemessene technische und organisatorische Maßnahmen ergriffen, um das Schutzniveau allzeit zu ermöglichen.

Hierbei werden insbesondere berücksichtig:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Insofern Subunternehmer für die Verarbeitung von Daten zum Einsatz kommen, wurden diese sorgfältig ausgewählt, insbesondere unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz. Sie wurden vor der Beauftragung und während der Vertragslaufzeit auf die Einhaltung der gesetzlichen und vertraglichen datenschutzrechtlichen Vorschriften sowie der vereinbarten technischen und organisatorischen Schutzmaßnahmen hin kontrolliert.

Um Daten vor Verlust, Beschädigung, unerlaubten Zugriff und unsachgemäßer Benutzung zu schützen, wird das Hogrefe Online-Portal in einem Rechenzentrum gehostet und verfügt über eine redundante Datenanbindung.

Zu den organisatorischen Maßnahmen gehören:

- Lückenlose Überwachung von Betrieb und Zutritt, rund um die Uhr.
- „Remote Hands“ sind zu den Geschäfts-/Supportzeiten verfügbar.
- Zutritt zum Rechenzentrum erhalten nur berechtigte Personen. Der Zugang zum Rechenzentrum kann dann per Zugangskarte und Zugangscode erfolgen.
  Das gesamte Rechenzentrum und das Gelände sind rund um die Uhr Video überwacht und die Überwachung wird ununterbrochen dokumentiert.
- Das Rechenzentrum verfügt über eine USV (Unterbrechungsfreie Stromversorgung) und kann damit auch im Falle längerer Stromausfälle von mehreren Stunden betrieben werden.
- Die Datenbanken werden kontinuierlich auf separater Hardware gesichert.

Die vollständige Liste der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO finden Sie unter IV. dieses Dokumentes.

## 6. Testschutz

Bitte beachten Sie, dass auch der Testschutz mit zum Datenschutz gehört. Wenn Tests für Fragestellungen eingesetzt werden, von denen eine Entscheidung abhängt, sollten die Items der Tests nicht öffentlich bekannt werden, da sonst Ergebnisse ggf. nicht verwendbar sind. Professionelle Testverfahren unterliegen kontrollierten Vertriebsbedingungen, die einen gewissen Schutz bieten. Dies gilt auch für PC-basierte Testverfahren. Wo immer möglich, sollten Sie wichtige Testdurchführungen unter kontrollierten Bedingungen durchführen. Dazu gehört

- die Identitätsprüfung der Person (bei prüfungsartigen Anlässen, wenn die Person nicht persönlich bekannt ist), ebenso
- wie die Beaufsichtigung der Testdurchführung (an entfernten Orten ggf. durch eine beauftragte Vertrauensperson und Verhinderung unerlaubter Hilfsmittel und Kommunikation).

# 7. Datenschutz-Folgeabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) ist ein Verfahren zur Sicherstellung und zum Nachweis der Einhaltung gesetzlicher Anforderungen. Art. 35 DSGVO verlangt eine DSFA, wenn die Form der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen hat. Dies kann sich insbesondere ergeben durch:

- die Verwendung neuer Technologien,
- der Art,
- den Umfang,
- der Umstände und
- der Zwecke

der Verarbeitung personenbezogener Daten. Anhand der Kriterien in Art. 35 DSGVO wird eine sog. Schwellenwertanalyse durchgeführt, um zu ermitteln, ob eine DSFA für die zu prüfende Verarbeitung durchzuführen ist. In folgenden Fällen ist der Schwellenwert stets überschritten und eine DSFA ist durchzuführen:

1. Die Form der Verarbeitung, insbesondere die Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung hat voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (Art. 35 Abs. 1 DSGVO).
2. Die Verarbeitung fällt unter eines der Regelbeispiele aus Art. 35 Abs. 3 DSGVO. Hierzu zählen:
    a. Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
    b. Die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art.9 Abs.1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art.10 DSGVO.
    c. Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
3. Die Verarbeitung befindet sich auf einer Liste nach Art. 35 Abs. 4 DSGVO.

Unter Umständen muss der Diagnostiker als datenschutzrechtlich Verantwortlicher für die Nutzung von HTS eine Datenschutz-Folgeabschätzung durchführen. Hogrefe als Auftragsverarbeiter ist nach Art. 28 Abs. 3 f) DSGVO verpflichtet, den Verantwortlichen bei der Durchführung der Datenschutz-Folgeabschätzung zu unterstützen.

Die genauen Umstände der Verarbeitung personenbezogener Daten durch den Diagnostiker im HTS und eventuell damit verbundene hohe Risiken für die Rechte und Freiheiten der betroffenen natürlichen Personen kann Hogrefe nicht antizipieren. Für die Datenschutz-Folgeabschätzung ist nicht nur der Verarbeitungsvorgang innerhalb des HTS, sondern auch Vorgänge, die außerhalb des HTS beim Diagnostiker im Rahmen der Durchführung der Tests stattfinden, von denen Hogrefe weder Kenntnis hat noch Einfluss darauf nehmen kann.

**Grundsätzlich ist es möglich, das HTS gänzlich ohne die Erfassung personenbezogener Daten zu nutzen, so dass ein hohes Risiko nahezu ausgeschlossen werden kann. Es ist andererseits auch möglich personenbezogene Daten sowie besondere Kategorien personenbezogener Daten innerhalb des HTS zu verarbeiten. Dies liegt in der Verantwortung des Diagnostikers.**

Sollte daher der Diagnostiker als datenschutzrechtlich Verantwortlicher zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sein, wird in diesem Dokument unter den Ziffern II. 2. bis 6. sowie IV. und V. eine Vielzahl von geeigneten Gegenmaßnahmen dargestellt, um etwaige Risiken auf ein adäquates Niveau zu senken. Diese Maßnahmen werden von Hogrefe kontinuierlich geprüft und weiterentwickelt. Es ist weder zu erwarten, dass hohe Risiken für die betroffenen Personen durch die Nutzung des HTS eintreten, noch dass eine Pflicht zur vorherigen Konsultation einer Aufsichtsbehörde nach Art. 36 DSGVO besteht, soweit die genannten Abhilfemaßnahmen durch den Diagnostiker ergriffen werden.

# III. Vertrag zur Auftragsverarbeitung



**Datenschutzvereinbarung nach Art. 28 DSGVO**
bzgl. der Erbringung von IT-Dienstleistungen

zwischen

_____ _____

Firma Ihre Kundennummer

_____

Straße / Hausnummer

_____

PLZ / Ort

(Verantwortlicher - nachfolgend **Auftraggeber** genannt)

und

der Hogrefe Verlag GmbH & Co. KG
Merkelstr. 3
37085 Göttingen

(Auftragsverarbeiter - nachfolgend **Auftragnehmer** genannt)

## Präambel

Dieser Vertrag konkretisiert entsprechend Art. 28 der EU-Verordnung 2016/679 (in Folgenden DSGVO) die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, bei der Erbringung von IT-Dienstleistungen.

Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

# 1. Definitionen

Es gelten die Definitionen des Art. 4 DSGVO.

# 2. Gegenstand, Umfang, Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen, Dauer

(1) Zweck des Auftrags ist die zwischen Verantwortlichem und Auftragnehmer bestehende Abrede über die Erbringung informationstechnischer Dienstleistungen, die mit Erwerb des Online-Portals in Kraft tritt. Bei der Erbringung informationstechnischer Dienstleistungen handelt es sich um eine weisungsgebundene Verarbeitung personenbezogener Daten seitens des Auftragnehmers für den Auftraggebers.

(2) Gegenstand dieser Abrede ist dabei insbesondere die Erbringung folgender Leistungen seitens des Auftragnehmers:

- Hosting des HTS Online-Portals und Gewährleistung der Lauffähigkeit
- Bereitstellung der Serverinfrastruktur zur Abwicklung von Online-Testungen
- Vorhalten der Testergebnisse in PDF-Form im Online-Portal, solange das Vertragsverhältnis andauert oder der Auftraggeber entsprechende Dateien eigenhändig löscht

(3) Im Rahmen der Erbringung der Dienstleistungen können folgende personenbezogene Daten betroffen sein:

- Name
- Alter
- Geschlecht
- E-Mail-Adresse (in Einzelfällen)
- Testergebnisse und Auswertungen

(4) Betroffen von der Datenverwendung können sein (abhängig vom Aufgabengebiet des Auftraggebers):

- ☐ Mitarbeiter
- ☐ Bewerber
- ☐ Coachees
- ☐ Patienten
- ☐ Sonstiges: _____

(5) Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

(6) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

# 3. Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO).

(2) Dem Auftragnehmer bleibt es vorbehalten, die personenbezogenen Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte personenbezogenen Daten nicht mehr als personenbezogene Daten im Sinne dieser Vereinbarung gelten.

(3) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung die entsprechenden rechtlichen Anforderungen mit.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

# 4. Datenschutzbeauftragter

Der Auftragnehmer hat einen externen betrieblichen Datenschutzbeauftragten benannt. Die Kontaktdaten des Datenschutzbeauftragten lauten:

Felix Hudy & Laura L. Stoll
Merkelstraße 3
D-37085 Göttingen
E-Mail: datenschutz@hogrefe.de

# 5. Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

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 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in Ziffer IV. „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(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 und dem Auftraggeber schriftlich mitzuteilen.

## 6. Verpflichtung auf die Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind 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.

## 7. Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Soweit betroffene Personen gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit ausüben können, stellt der Aufragnehmer sicher, dass sie die Daten, die sie dem Auftraggeber bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten können.

(3) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(4) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

## 8. Unterstützung bei Dokumentations- und Meldepflichten

(1) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(2) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen

## 9. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der getroffenen technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und den datenschutzrechtlichen Vorgaben selbst oder durch einen anderen von diesem beauftragten Prüfer zu kontrollieren.
Hierfür kann er alternativ

- Selbstauskünfte des Auftragnehmers einholen oder
- sich ein vorhandenes Testat eines externen Sachverständigen oder des betrieblichen Datenschutzbeauftragten vorlegen lassen oder
- sich im Falle eines begründeten Zweifels an den vorgelegten Unterlagen oder eines datenschutzrechtlich relevanten Vorfalls, nach rechtzeitiger Anmeldung unter Angabe der Gründe, zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs, persönlich überzeugen (Audit).

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggebers alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(3) Der Auftragnehmer ist verpflichtet, Kontrollen des Auftraggebers im Hinblick auf die Einhaltung dieser Vereinbarung und die damit einhergehende Einhaltung datenschutzrechtlicher Vorschriften, insbesondere durch die Einholung von Auskünften zu dulden. Der Auftragnehmer wird auf Anfragen des Auftraggebers unverzüglich auf den konkreten Einzelfall bezogene Auskunft erteilen und bei Kontrollen die Einhaltungen dieses Vertrages auf Aufforderung durch geeignete Nachweise belegen.

## 10. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Subunternehmer einzubeziehen. Zehn Wochen vor Hinzuziehung eines Subunternehmers informiert der Auftragnehmer den Auftraggeber. Die durch den Auftraggeber zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in der unter Ziffer V. dieser Vereinbarung aufgelistet. Als Subunternehmer im Sinne dieser Regelung gelten Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt.

(2) Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines Subunternehmers zu erheben. Der Auftraggeber wird das Einspruchsrecht nur aus sachlichem Gründen unter Berücksichtigung billigen Ermessens unverzüglich, spätestens innerhalb einer Frist von 2 Wochen nach Erhalt der Information, ausüben. Der Einspruch muss in Textform erfolgen und sämtliche Gründe nennen, die einer Beauftragung des Subauftragnehmers nach Auffassung des Auftraggebers entgegenstehen. Für den Fall, dass der Einsatz des Subauftragnehmers erforderlich ist, um das Risiko einer wesentlichen Beeinträchtigung der Interessen einer Vertragspartei oder der betroffenen Personen auszuschließen, ist der jeweilige Auftragnehmer berechtigt, den Subunternehmer, über dessen Einsatz der Auftraggeber informiert wurde, schon vor Ablauf der Einspruchsfrist vorläufig einzusetzen. Der vorläufige Einsatz des Subunternehmers endet in diesen Fällen mit einem Einspruch des Auftraggebers, der billigem Ermessen und den vorgenannten Anforderungen an Form und Begründung entspricht. Wesentliche Beeinträchtigungen im Sinne der vorstehenden Regelung liegen z. B. vor, wenn die Hinzuziehung eines Subunternehmers aus Gründen der Datensicherheit geboten ist oder ohne den Einsatz des Subunternehmers dem Auftragsverarbeiter ein unverhältnismäßig hoher Aufwand oder Schaden entstünde.

(3) Subunternehmer sind sorgfältig auszuwählen, insbesondere unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz im Sinne von Art. 32 DSGVO. Sie sind vor der Beauftragung und während der Vertragslaufzeit auf die Einhaltung der gesetzlichen und vertraglichen datenschutzrechtlichen Vorschriften sowie der vereinbarten technischen und organisatorischen Schutzmaßnahmen hin zu kontrollieren. Die Ergebnisse dieser Kontrolle sind zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(4) Vertragliche Vereinbarungen zwischen dem Auftragnehmer und Subunternehmern haben den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung zu entsprechen. Die Übermittlung von personenbezogenen Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen aus Art. 28 DSGVO erfüllt.

(5) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

## 11. Löschung und Herausgabe

(1) Der Auftragnehmer wird die personenbezogenen Daten nur solange aufbewahren, wie vom Auftraggeber angewiesen. Sofern keine konkrete Weisung vorliegt, werden die personenbezogenen Daten vor der Vernichtung nur solange aufbewahrt, wie dies zur Durchführung der jeweiligen Auftragsverarbeitung unter dieser Vereinbarung notwendig ist.

(2) Auf Verlangen des Auftraggebers sowie nach Beendigung dieser Vereinbarung wird der Auftragnehmer sämtliche personenbezogenen Daten, die im Zusammenhang mit dieser Auftragsverarbeitung stehen, sowie etwaige Kopien davon unverzüglich, spätestens jedoch binnen 14 Tagen nach Aufforderung und Weisung des Auftraggebers bzw. Beendigung der Auftragsverarbeitung, unter Einhaltung einschlägiger datenschutzrechtlicher Bestimmungen löschen.

(3) Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Der Auftragnehmer weist dem Auftraggeber die Löschung auf Verlangen schriftlich nach.

## 12. Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

(2) Der Auftragnehmer ist zum Zwecke der Enthaftung gem. Art. 82 Abs. 3 DSGVO dazu befugt, Details zu Weisungen des Auftraggebers und zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber ist dazu verpflichtet, den Auftragnehmer bestmöglich zu unterstützen, damit sich der Auftragnehmer gegenüber dem Dritten nach Art. 82 Abs. 3 DSGVO enthaften kann.

(3) Etwaige Haftungserleichterungen im Verhältnis des Auftraggebers zur betroffenen Person wirken auch zugunsten des Auftragnehmers, sodass sich ein etwaiger Erstattungsanspruch gegen den Auftragnehmer um den Anteil reduziert, den der Auftraggeber aufgrund der Haftungserleichterung im Außenverhältnis erspart.

(4) Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

## 13. Sonstige Bestimmungen

(1) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(2) Sollten einzelne oder mehrere Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so bleibt die Wirksamkeit der Vereinbarung im Übrigen davon unberührt. An die Stelle der unwirksamen Regelung(en) soll jeweils eine Bestimmung treten, die in ihrem wirtschaftlichen Ergebnis demjenigen möglichst nahekommt, welches die Parteien mit der unwirksamen Regelung angestrebt hatten. Entsprechendes gilt im Fall von Vertragslücken.

| | |
|---|---|
| _____<br>Ort, Datum<br><br>_____<br>Unterschrift, Stempel Verantwortlicher | Göttingen, den 08.04.2024<br>Ort, Datum<br><br>_____<br>Unterschrift, Stempel Auftragnehmer |

# IV. Technisch-organisatorische Maßnahmen

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

### (1) Zutrittskontrolle

**Regelungsgegenstand**

Die Zutrittskontrolle soll verhindern, dass sich Unbefugte den Anlagen der Datenverarbeitung räumlich nähern und so physischen Zugriff auf die Systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, bekommen. Bei der Zutrittskontrolle werden deshalb verschiedene bauliche, organisatorische und personelle Maßnahmen getroffen und in einem Zutrittskontrollkonzept geregelt.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen verhindern, dass unbefugte Zutritt zu Datenverarbeitungsanlagen haben:

- Berechtigungsausweise
- Elektronische Zutrittscodekarten/ Zutrittstransponder
- Zutrittsberechtigungskonzept
- Videoüberwachung
- Alarmanlage
- Schlüsselregelung
- Begleitung von Besucherzutritten durch eigene Mitarbeiter
- Anwesenheitsaufzeichnungen von Besucherzutritten
- Abgestufte Sicherheitsbereiche und kontrollierter Zutritt
- Gesondert gesicherter Zutritt zum Rechenzentrum
- Aufbewahrung der Server in verschlossenen Räumen
- Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen
- Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe

### (2) Zugangskontrolle

**Regelungsgegenstand**

Die Zugangskontrolle soll verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Hierbei soll durch geeignete Maßnahmen gewährleisten werden, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung haben. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert die Zugangskontrolle den Zugriff auf das IT-System.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen verhindern, dass unbefugte Zugang zu Datenverarbeitungsanlagen haben:

- Passwortsicherung von Bildschirmarbeitsplätzen
- Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- Verwendung von individuellen Passwörtern
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
- Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität:
  - Mindestens 8 Ziffern / Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)
  - Verhinderung von Trivialpasswörtern (z.B. Hund1, Hund2, Hund3)
  - Passworthistorie (keine erneute Verwendung der letzten 5 Passwörter)
- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern

- Verpflichtung zur Vertraulichkeit
- Protokollierung und Auswertung der Systembenutzung
- Kontrollierte Vernichtung von Datenträgern

## (3) Zugriffskontrolle

**Regelungsgegenstand**

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen verhindern, dass Unbefugte Zugriff zu Datenverarbeitungsanlagen haben:

- Festlegung der Zugriffsberechtigung, Berechtigungskonzept
- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
- Regelmäßige Überprüfung von Berechtigungen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Regelmäßige Auswertung von Protokollen (Logfiles)
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
- Protokollierung von Dateizugriffen
- Protokollierung von Dateilöschungen
- Es werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt:
  - Virenscanner
  - Firewalls
  - SPAM-Filter
  - Intrusionprevention (IPS)
  - Intrusiondetection (IDS)
- Verschlüsselte Speicherung der Daten
- Verwendung von Hash-Funktion - SHA2 (256, 384, 512 bit)

## (4) Trennungskontrolle

**Regelungsgegenstand**

Die Trennungskontrolle soll gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Grund dafür ist u.a. die Zuordenbarkeit der Daten zu einer bestimmten Abteilung, Person, Zweigstelle oder Kunden, aber auch die Erfüllung des datenschutzrechtlichen Grundprinzips der zweckgebundenen Nutzung von Daten. Dabei kann das Ziel auf vielfältige Weise erreicht werden. Bspw. durch ein geeignetes Rollen- und Berechtigungskonzept innerhalb von Anwendungen.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
- Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern des Auftragnehmers
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
- Funktionstrennung
- Trennung von Entwicklungs-, Test- und Produktivsystem
- dediziertes System

### (5) Pseudonymisierung

Der Auftraggeber kann entsprechende Einstellungen im System vornehmen, damit die Verarbeitung personenbezogener Daten in einer Weise erfolgt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### (1) Weitergabekontrolle

**Regelungsgegenstand**
Die Weitergabekontrolle soll gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

**Technische und organisatorische Maßnahmen**
Folgende Maßnahmen sind zur Sicherstellung implementiert:

- Datenaustausch erfolgt über https-Verbindung
- Sicheres Vernichten von Papierdokumenten durch Nutzung verschlossener Behältnisse aus Metall (sog. Datenschutztonnen) und dokumentierter Entsorgung durch Dienstleister

### (2) Eingabekontrolle

**Regelungsgegenstand**
Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

**Technische und organisatorische Maßnahmen**
Folgende Maßnahmen sind zur Sicherstellung implementiert:

- Kennzeichnung erfasster Daten
- Festlegung von Benutzerberechtigungen (Profile)
- Differenzierte Benutzerberechtigungen:
  - Lesen, Ändern, Löschen
  - Teilzugriff auf Daten bzw. Funktionen
  - Feldzugriff bei Datenbanken
- Organisatorische Festlegung von Eingabezuständigkeiten
- Protokollierung von Eingaben/Löschungen
- Verpflichtung auf das Datengeheimnis
- Über OS-Standard hinausgehendes Log-Konzept

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### (3) Verfügbarkeitskontrolle

**Regelungsgegenstand**
Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen sind zur Sicherstellung implementiert:

- Datensicherungs- und Backupkonzepte
- Durchführung der Datensicherungs- und Backupkonzepte
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
- Brandmeldeanlagen in Serverräumlichkeiten
- Rauchmelder in Serverräumlichkeiten
- Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten
- Klimatisierte Serverräumlichkeiten
- Blitz-/ Überspannungsschutz
- Wassersensoren in Serverräumlichkeiten
- Serverräumlichkeiten in separaten Brandabschnitt
- Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt
- Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
- CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten
- Aufbewahrung der Daten in Datensicherungsschränken, Tresoren
- USV-Anlage (Unterbrechungsfreie Stromversorgung)

## (4) Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

**Regelungsgegenstand**

Die Widerstandsfähigkeit- und Ausfallsicherheitskontrolle soll gewährleisten, dass Systeme die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen sind zur Sicherstellung implementiert:

- Redundante Stromversorgung
- Redundante USV-Anlage
- Redundante Klimatisierung
- Festplattenspiegelung
- Datenspeicherung auf RAID-Systemen (RAID 1 und höher)
- Abgrenzung kritischer Komponenten
- Durchführung von Penetrationstests
- Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
- Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
    - Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.
    - Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.
    - Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).
    - Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden.
    - Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.
    - Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.

- Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst:
  - Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.
  - Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.
- Periodische Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind.

# 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

## (5) Kontrollverfahren

Folgende Maßnahmen sind zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen implementiert:

- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen

## (6) Auftragskontrolle

**Regelungsgegenstand**

Die Auftragskontrolle soll gewährleisten, dass Daten die im Auftrag durch Dienstleister (Subunternehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.

**Technische und organisatorische Maßnahmen**

Folgende Maßnahmen sind zur Sicherstellung implementiert:

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
- Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)
- Vor-Ort-Kontrollen beim Auftragnehmer
- Überprüfung des Datensicherheitskonzepts beim Auftragnehmer
- Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer

# V. Liste der Subunternehmer

Die nachfolgenden Subunternehmer werden bei der Verarbeitung hinzugezogen, jedoch nur unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO:

| Firma (Subunternehmer) und Anschrift | Verarbeitungsstandort | Art der Dienstleistung | Beginn der Dienstleistung |
|---|---|---|---|
| Hogrefe Digital Solutions GmbH<br>Merkelstr. 3<br>37085 Göttingen | Göttingen, Deutschland | Hosting, Betrieb, Support und Entwicklung des HTS Online-Portals | **01. Juli 2024** |

# VI. Übersicht der Verarbeitungstätigkeit gem. Artikel 30 Abs. 2 DSGVO

| | |
|---|---|
| **Angaben zum Auftragsverarbeiter** | |
| Firmengruppe | ☒ ja ☐ nein |
| Name | Hogrefe Verlag GmbH & Co. KG |
| Straße | Merkelstraße 3 |
| Postleitzahl | 37085 |
| Ort | Göttingen |
| Telefon | 49 (0)551 999 50-880 |
| E-Mail-Adresse | e-tests@testzentrale.de |
| Internet-Adresse | www.testzentrale.de |
| **Angaben zur Person des Datenschutzbeauftragten** | |
| Anrede | Herr |
| Name, Vorname | Hudy, Felix |
| Straße | Merkelstraße 3 |
| Postleitzahl | 37085 |
| Ort | Göttingen |
| Telefon | 49 (0)40 790 235 0 |
| E-Mail-Adresse | datenschutz@hogrefe.de |
| Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden<br>(Art. 30 Abs. 2 lit. b) | • Hosting des HTS Online-Portals und Gewährleistung der Lauffähigkeit<br>• Bereitstellung der Serverinfrastruktur zur Abwicklung von Online-Testungen<br>• Vorhalten der Testergebnisse in PDF-Form im Online-Portal, solange das Vertragsverhältnis andauert oder der Auftraggeber entsprechende Dateien eigenhändig löscht |
| ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation<br>(Art. 30 Abs. 2 lit. c) | ☒ Datenübermittlungen finden nicht statt und sind auch nicht geplant |
| Subunternehmer | **Ab dem 01. Juli 2024**<br>Hogrefe Digital Solutions GmbH<br>Merkelstr. 3<br>37085 Göttingen<br><br>Datenschutzbeauftragte Felix Hudy & Laura L. Stoll<br>datenschutz@hogrefe.de<br><br>Art der Dienstleistung: Hosting, Betrieb, Support und Entwicklung des HTS Online-Portals |