hogrefe

Datenschutz bei Hogrefe

Verantwortungsvoller Umgang mit sensiblen Daten

Version: 1.8

Hogrefe Verlag

Merkelstraße 3
37085 Göttingen
Germany

Tel. +49 551 999 50 0
Fax +49 551 999 50 111
verlag@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@hogrefe.de
Internet: www.testzentrale.de

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

Felix Hudy
Managing Consultant Datenschutz
Externer betrieblicher Datenschutzbeauftragter 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:

1. Schutz personenbezogener Daten vor Missbrauch
2. Schutz elektronischer Daten gegen Verlust oder Veränderung
3. 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.

Daten auf den Servern werden 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 SSL-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 (Passwortwechsel).

4. EU-Datenschutzgrundverordnung (DSGVO)

Das HTS erfüllt die datenschutzrechtlichen Anforderungen der DSGVO. 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 V. die Übersicht von Verarbeitungstätigkeiten gem. Artikel 30 Abs. 2 DSGVO dargestellt.

Alle Mitarbeiter sind mit den Anforderungen der DSGVO vertraut gemacht worden und auf die Vertraulichkeit verpflichtet.

5. Schutz elektronischer Daten gegen Verlust oder Veränderung

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 im Anhang des Vertragsentwurfes unter II.

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).

III. Vertrag zur Auftragsdatenverarbeitung

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

zwischen

Kundendaten
(Firma, Adresse, 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 Datenverwendung, Kreis der Betroffenen, 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 haben die Mitarbeiter des Auftragnehmers Zugang zu folgenden Daten der Betroffenen:

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

(4) Beschränkt auf den Zweck der ordnungsgemäßen Erbringung o.g. IT-Dienstleistungen darf der Auftragnehmer personenbezogene Daten für den Auftraggebers erheben, speichern, verändern, übermitteln und nutzen.

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

- Mitarbeiter
- Bewerber
- Coachees
- Patienten
- Sonstiges: .....

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

(7) Die Verarbeitung der personenbezogenen 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, personenbezogene 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.

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) Der Auftragnehmer darf die personenbezogenen Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet diese Vereinbarung keine Anwendung.

(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. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der personenbezogenen Daten beim Auftraggeber liegt.

4. Datenschutzbeauftragter

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

Felix Hudy
Managing Consultant Datenschutz
Merkelstraße 3
D-37085 Göttingen
E-Mail: datenschutz@hogrefe.de

5. Technische und organisatorische Schutzmaßnahmen

(1) Der Auftragnehmer gewährleistet die Umsetzung der im Rahmen der ordnungsgemäßen Durchführung der Auftragsarbeiten erforderlichen Sicherheitsmaßnahmen. Er trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten, die den Anforderungen der Datenschutzgrundverordnung, insbesondere Art. 32 DSGVO, genügen. Hierzu 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
- die in der Anlage zu dieser Vereinbarung abgebildeten Maßnahmen treffen.

(2) Der Auftragnehmer unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3) Die erforderlichen 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 mitzuteilen.

6. Verpflichtung auf die Vertraulichkeit

(1) Der Auftragnehmer ist verpflichtet, bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit gemäß Art. 28 Abs. 3 b) DSGVO zu wahren. Insbesondere hat er zu gewährleisten, dass die aus dem Bereich des Auftraggebers erlangten personenbezogenen Daten nicht an Dritte weitergegeben oder auf andere Art verwertet werden. Er darf bei der Verarbeitung und Nutzung der personenbezogenen Daten des Auftraggebers nur Beschäftigte einsetzen, die gemäß Art. 28 Abs. 3 b) DSGVO schriftlich auf die Vertraulichkeit verpflichtet sind.

(2) Der Auftragnehmer hat die mit der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und die Einhaltung der datenschutzrechtlichen Vorschriften durch die Mitarbeiter zu überwachen. Die regelmäßige Schulung der Mitarbeiter hat er zu dokumentieren und diese auf Verlangen dem Auftraggeber zur Verfügung zu stellen.

7. Informationspflichten

(1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die dieser benötigt, um die Einhaltung der Vorschriften zur Auftragsverarbeitung gemäß Art. 28 DSGVO dokumentieren und nachweisen zu können.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich über datenschutzrelevante Betriebsstörungen, bei Indizien für mögliche oder feststehende Datenschutzverletzungen, bei sonstigen Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers sowie bei Verstößen gegen die Bestimmung dieser Vereinbarung durch den Auftragnehmer oder etwaiger Subunternehmer des Auftragnehmers. Etwaige Mängel bei der Auftragsverarbeitung sind unverzüglich und unter Erbringung eines schriftlichen Nachweises vom Auftragnehmer zu beseitigen.

(3) Der Auftragnehmer stellt dem Auftraggeber die für das Verzeichnis aller Verarbeitungstätigkeiten nach Art. 30 DSGVO notwendigen Informationen zur Verfügung.

(4) Sollten personenbezogene Daten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu informieren. Der Auftragnehmer wird die in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten bei dem Auftraggeber liegt.

8. Sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer ermöglicht eine ordnungsgemäße Datenschutzkontrolle und Aufsicht durch die zuständige Aufsichtsbehörde. Insbesondere erteilt er der Aufsichtsbehörde richtig, vollständig und rechtzeitig Auskunft, duldet Prüfungen und Kontrollmaßnahmen und vollzieht Anordnungen der Aufsichtsbehörde. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls sich die Aufsichtsbehörde im Rahmen ihrer Datenschutzkontrolle und Aufsicht unmittelbar an den Auftragnehmer wenden sollte.

(2) Der Auftragnehmer stellt sicher, dass der Auftraggeber gesetzliche Ansprüche Betroffener aus den Art. 12 bis 22 DSGVO erfüllen kann. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zu treffen, um den Auftraggeber bei der Beantwortung entsprechender Anträge von Betroffenen zu unterstützen. Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls sich ein Betroffener zum Zwecke der Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder Übertragung seiner Daten unmittelbar an den Auftragnehmer wenden sollte.

(3) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei den zu treffenden Maßnahmen in Bezug auf die Datensicherheit nach Art. 32 DSGVO, bei gegebenenfalls nötigen Meldungen an die Aufsichtsbehörde (Art. 33 DSGVO) oder bei Benachrichtigungen Betroffener (Art. 34 DSGVO), bei der

Durchführung von Datenschutz-Folgeabschätzungen (Art. 35 DSGVO) sowie bei der Abstimmung mit Aufsichtsbehörden (Art. 36 DSGVO) zu unterstützen. Insbesondere bei der Erfüllung der Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) wird der Auftragnehmer dem Auftraggeber die notwendigen Informationen unverzüglich zur Verfügung stellen.

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). Die mit einem Audit verbundenen Kosten trägt der Auftraggeber.

(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) Zum Zeitpunkt des Vertragsschlusses werden keine Subunternehmer eingesetzt. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter einzubeziehen. Zehn Wochen vor Hinzuziehung eines Subunternehmers informiert der Auftragnehmer den Auftraggeber. Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen 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 weiteren Auftragsverarbeiters zu erheben. Der Auftraggeber wird das Einspruchsrecht im Hinblick auf den jeweiligen Auftragnehmer 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) Sollten die EU-Kommission oder die zuständige Aufsichtsbehörde Standardklauseln für Auftragsverarbeitungsverträge festlegen, werden sich die Parteien im erforderlichen Umfang auf eine mögliche Anpassung dieser Vereinbarung an die Standardklauseln verständigen.

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

(3) 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 nahe kommt, welches die Parteien mit der unwirksamen Regelung angestrebt hatten. Entsprechendes gilt im Fall von Vertragslücken.

_____ Ort, Datum _____ Unterschrift, Stempel Verantwortlicher	_____ Ort, Datum _____ Unterschrift, Stempel Auftragnehmer

IV. Übersicht von Verarbeitungstätigkeiten Auftragnehmer 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@hogrefe.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	datenschutzy@hogrefe.de

Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden (Art. 30 Abs. 2 lit. b)	• 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
ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 2 lit. c)	☒ Datenübermittlungen finden nicht statt und sind auch nicht geplant
Subunternehmer	☒ Subunternehmer werden nicht eingesetzt