hogrefe

Datenschutz bei Hogrefe

Verantwortungsvoller Umgang mit sensiblen Daten

Version: 1.6

Testzentrale der Schweizer Psychologen AG

Länggass-Strasse 76
3012 Bern
Schweiz

Tel. +41 31 300 45 45
Fax +41 31 300 45 90
hts@hogrefe.ch
www.testzentrale.ch

Inhalt

I. Kontaktinformation 5
II. Allgemeine Hinweise zum Hogrefe-Datenschutz 6
1. Erläuterung zum Datenschutz im Hogrefe Testsystem (Online-Portal) 6
2. Allgemein 6
3. Schutz personenbezogener Daten vor Missbrauch 7
4. EU-Datenschutzgrundverordnung (DSGVO) 7
5. Schutz elektronischer Daten gegen Verlust oder Veränderung 7
6. Testschutz 8
III. Vertrag zur Auftragsdatenverarbeitung 9
1. Definitionen 9
2. Gegenstand, Umfang, Art und Zweck der Datenverwendung, Kreis der Betroffenen 9
3. Verantwortung für die rechtliche Zulässigkeit 10
4. Weisungsgebundenheit des Auftragsverarbeiters 10
5. Datenschutzbeauftragter 11
6. Technische und organisatorische Schutzmaßnahmen 11
7. Verpflichtung auf die Vertraulichkeit 12
8. Informationspflichten 12
9. Sonstige Pflichten des Auftragsverarbeiters 12
10. Kontrollrechte des Verantwortlichen 13
11. Subunternehmer 14
12. Löschung und Herausgabe 14
13. Haftung 15
14. Sonstige Bestimmungen 15
IV. Technisch-organisatorische Maßnahmen 16
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 16
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 18
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 18
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) 20
V. Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter gem. Artikel 30 Abs. 2 DSGVO 21

I. Kontaktinformation

Testzentrale der Schweizer Psychologen AG
Länggass-Strasse 76
3012 Bern
Schweiz
Tel: +41 (0)31 300 45 45
FAX: +41 (0)31 300 45 90
E-Mail: hts@hogrefe.ch
Internet: www.testzentrale.ch

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

Felix Hudy
Managing Consultant Datenschutz
Externer betrieblicher Datenschutzbeauftragter bei Hogrefe
Merkelstraße 3
37085 Göttingen
Deutschland
E-Mail: privacy@hogrefe.com

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; einzelne Ergebnisse können gelöscht werden, wenn man sie dort über die Detail-Ansicht aufruft. 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 des Auftragsverarbeiters 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)

(nachfolgend **Verantwortlicher** genannt)

und

der Testzentrale der Schweizer Psychologen AG
Länggass-Strasse 76
3012 Bern

(nachfolgend **Auftragsverarbeiter** 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 Auftragsverarbeiters oder durch ihn beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

1. Definitionen

Es gelten die Definitionen des Art. 4 DSGVO.

2. Gegenstand, Umfang, Art und Zweck der Datenverwendung, Kreis der Betroffenen

(1) Zweck des Auftrags ist die zwischen Verantwortlichem und Auftragsverarbeiter 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 Auftragsverarbeiters für den Verantwortlichen.

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

- 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 Verantwortliche entsprechende Dateien eigenhändig löscht

(3) Im Rahmen der Erbringung der Dienstleistungen haben die Mitarbeiter des Auftragsverarbeiters 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 Verantwortlichen erheben, speichern, verändern, übermitteln und nutzen.

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

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

3. Verantwortung für die rechtliche Zulässigkeit

(1) Der Verantwortliche ist aufgrund seiner Eigenschaft aus Art. 4 Nr. 7 DSGVO allein verantwortlich für die Beurteilung der rechtlichen Zulässigkeit, der im Rahmen des Auftragsverhältnisses durchgeführten Verarbeitung und Nutzung personenbezogener Daten durch den Auftragsverarbeiter, im Hinblick auf die Regelungen der DSGVO, des BDSG und anderer Vorschriften über den Datenschutz.

(2) Aufgrund dieser Verantwortung kann der Verantwortliche auch während der Laufzeit und nach Beendigung des Vertrages Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

(3) Allein dem Verantwortlichen obliegt die Prüfung hinsichtlich der rechtlichen Zulässigkeit bestimmter von ihm durchgeführter oder geplanter Verarbeitungstätigkeiten.

4. Weisungsgebundenheit des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet und nutzt die personenbezogenen Daten des Verantwortlichen ausschließlich im Rahmen der vereinbarten Leistungserbringung und der speziellen Einzelweisungen des Verantwortlichen. Der Auftragsverarbeiter ist nicht berechtigt, die personenbezogenen Daten des Verantwortlichen in einer anderen als der angewiesenen und unter Ziff. 2 genannten Weise zu erheben, verarbeiten oder zu nutzen.

(2) Der Verantwortliche oder ein Bevollmächtigter des Verantwortlichen wird Weisungen, die von der Vereinbarung nach Ziff. 2 abweichen, schriftlich per Brief, Fax oder E-Mail erteilen. Mündliche Weisungen werden per Brief, Fax oder E-Mail umgehend bestätigt.

(3) Eine Berichtigung, Löschung oder Sperrung von Daten ist dem Auftragsverarbeiter nicht gestattet, es sei denn, es liegt eine entsprechende schriftliche Weisung des Verantwortlichen vor.

5. Datenschutzbeauftragter

Der Auftragsverarbeiter 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

6. Technische und organisatorische Schutzmaßnahmen

(1) Der Auftragsverarbeiter 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 Auftragsverarbeiter:

- 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 Auftragsverarbeiter 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 Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen mitzuteilen.

(4) Dem Verantwortlichen sind die vom Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen bekannt. Der Verantwortliche trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(5) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Dokumentation der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen.

7. Verpflichtung auf die Vertraulichkeit

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

(2) Der Auftragsverarbeiter 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 Verantwortlichen zur Verfügung zu stellen.

8. Informationspflichten

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

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

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

9. Sonstige Pflichten des Auftragsverarbeiters

(1) Für andere als die in Ziff. 2 dieser Vereinbarung festgelegten Zwecke dürfen die personenbezogenen Daten nur mit schriftlicher Zustimmung des Auftraggebers verarbeitet werden. Dies gilt insbesondere für eine Weitergabe an Dritte.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen die DSGVO, das BDSG oder andere datenschutzrechtliche Vorschriften der Europäischen Union oder der Mitgliedstaaten verstößt, weist der Auftragsverarbeiter den Verantwortlichen unverzüglich hierauf hin.

(3) Bei gesetzlichen Ausnahmen von der Weisungsgebundenheit des Auftragsverarbeiters gemäß Art. 28 Abs. 3 S. 2 a) DSGVO informiert der Auftragsverarbeiter den Verantwortlichen über auf Grundlage von Rechtsvorschriften erfolgte oder unterbliebene Datenverarbeitungen, es sei denn, die Rechtsvorschrift verbietet dem Auftragsverarbeiter eine Mitteilung.

(4) Der Auftragsverarbeiter hält die für ihn geltenden datenschutzrechtlichen Bestimmungen ein. Insbesondere wird der Auftragsverarbeiter nicht Daten, die nicht allgemein zugänglich sind, unbefugt verarbeiten, zum Abruf mittels automatisierter Verfahren bereithalten, abrufen oder sich oder einem anderen aus automatisierter Verarbeitungen oder nicht automatisierten Dateien verschaffen.

(5) Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften dieser Vereinbarung und der Weisungen des Auftraggebers regelmäßig während der gesamten Vertragslaufzeit.

(6) Der Auftragsverarbeiter 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 Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, falls sich die Aufsichtsbehörde im Rahmen ihrer Datenschutzkontrolle und Aufsicht unmittelbar an den Auftragsverarbeiter wenden sollte.

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

(8) Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen 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.

10. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und dokumentiert das Ergebnis.
Hierfür kann er alternativ

- Selbstauskünfte des Auftragsverarbeiters 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 Verantwortliche.

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

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

11. Subunternehmer

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmer) ohne vorherige gesonderte Genehmigung des Verantwortlichen beauftragen.

(2) 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 Verantwortlichen zu übermitteln.

(3) Vertragliche Vereinbarungen zwischen dem Auftragsverarbeiter 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.

(4) Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche die Prüfungsrechte nach Ziff. 10 dieser Vereinbarung auch gegenüber Subunternehmern hat, die der Auftragsverarbeiter einsetzt.

(5) Der Verantwortliche ist berechtigt, beim Auftragsverarbeiter Einsicht in dessen Verträge mit Subunternehmern zu nehmen und vom Auftragsverarbeiter die Übersendung einer Kopie dieser Verträge zu verlangen.

12. Löschung und Herausgabe

(1) Der Auftragsverarbeiter wird die personenbezogenen Daten nur solange aufbewahren, wie vom Verantwortlichen 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 Auftragsverarbeiter 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 Auftragsverarbeiter entsprechend den jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

(4) Der Auftragsverarbeiter weist dem Verantwortlichen die Löschung auf Verlangen schriftlich nach.

13. Haftung

(1) Der Auftragsverarbeiter haftet dem Verantwortlichen für Schäden, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Dies gilt nicht, wenn der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten die Pflichtverletzung nicht zu vertreten haben. Dies gilt ebenfalls nicht, wenn der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten den verursachten Schaden nicht zu vertreten haben.

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

(3) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem Gesetz oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Verantwortliche gegenüber den Betroffenen verantwortlich.

14. 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	Ort, Datum
_____	_____
Unterschrift, Stempel Verantwortlicher	Unterschrift, Stempel Auftragsverarbeiter

IV. Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(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 DS-GVO)

(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 DS-GVO)

(1) 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)

(2) 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 DS-GVO; Art. 25 Abs. 1 DS-GVO)

(1) 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

(2) Auftragskontrolle

Regelungsgegenstand

Die Auftragskontrolle soll gewährleisten, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) 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. Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter gem. Artikel 30 Abs. 2 DSGVO

Angaben zum Auftragsverarbeiter

Firmengruppe	☒ ja ☐ nein
Name	Testzentrale der Schweizer Psychologen AG
Straße	Länggass-Strasse 76
Postleitzahl	3012
Ort	Bern
Telefon	41 (0)31 300 45 45
E-Mail-Adresse	hts@hogrefe.ch
Internet-Adresse	www.testzentrale.ch

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	privacy@hogrefe.com

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 Verantwortliche 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