Anlage 2: Technische und organisatorische Maßnahmen der gepedu GmbH gemäß Art. 32 DSGVO „Sicherheit der Verarbeitung“ Stand: 12.02.2020

Die gepedu trifft verschiedenste technische und organisatorische Maßnahmen, um ein dem Stand der Technik und dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese technischen und organisatorischen Maßnahmen werden einmal pro Quartal einer Prüfung durch die für die Datenverarbeitung bei der gepedu verantwortlichen Personen in Zusammenarbeit mit dem Datenschutzbeauftragten der gepedu unterzogen und gegebenenfalls aktualisiert.

1. Maßnahmen zur Sicherung der Vertraulichkeit

1.1. Zutrittskontrolle

Die zentrale Datenbank sowie der Mailserver der gepedu befinden sich in einem deutschen Rechenzentrum (zum Hoster siehe Anlage 1). Dieses Rechenzentrum verfügt über die notwendigen technischen und organisatorischen Maßnahmen zur Zutrittskontrolle, welche im Dokument „Domainfactory_TOM_V1.1.pdf“ bzw. in einer neueren Version dieses Dokuments beschrieben werden. Die aktuelle Fassung sendet Ihnen die gepedu auf Anfrage gerne zu.

1.2 Zugangskontrolle

Auf die serverbasierten Datenbanken (Webserver) kann von verschiedenen Seiten zugegriffen werden:

1.2.1 Kundenbereich

Der Kundenbereich ist nur registrierten Kunden/Auftraggebern der gepedu per Webformular zugänglich. Zum Login bedarf es eines Authentifikation mittels Benutzernamen und Passwort. Bei mehrmaliger Falscheingabe des Passworts wird der zugehörige Account gesperrt. Alle Webseiten des Kundenbereichs sind per https verschlüsselt.
Für jeden Account können verschiedene Rechte vergeben werden. „Standardaccounts“ können nur auf solche Teilnehmerdaten zugreifen, die zu den von ihnen generierten Zugangscodes gehören. Ein Auftraggeber mit mehreren Accounts kann auch „Masteraccounts“ besitzen, die wiederrum die Standardaccounts administrieren können.

1.2.2 Zugriff auf die serverbasierten Datenbanken durch die gepedu

Die Endgeräte der gepedu können ortsunabhängig mittels passwortgeschützter und verschlüsselter Verbindungen auf die Datenbanken und Dateien des Webservers zugreifen. Dazu werden Technologien wie sFTP, SSH und https (SSL) verwendet. Der Server der gepedu besitzt dafür ein eigenes Sicherheitszertifikat, welches von der Firma GlobalSign ausgestellt und jährlich erneuert/verlängert wird.

1.2.3 Schutz der lokalen Endgeräte der gepedu

Die Datenverarbeitung durch die Mitarbeiter der gepedu findet ausschließlich in elektronischer Form statt. Es werden keine Ausdrucke von fertigen Auswertungen oder von Rohdatensätzen in Papierform erstellt. Alle Endgeräte und Datenspeicher der gepedu sind mittels Passwort und Verschlüsselung vor unbefugtem Zugang geschützt. Als Technologien kommen hier beispielsweise Microsoft Bitlocker mit TPM-Modul und VeraCrypt zum Einsatz. Auf mobilen Endgeräten kann die Passworteingabe durch biometrische Verfahren ergänzt werden (Fingerabdruckscanner).
Des Weiteren sind die Endgeräte durch eine Antivirensoftware und eine Software-Firewall geschützt. An den Standorten der gepedu ist zusätzlich die Firewall des Internetrouters aktiv.

1.3 Zugriffskontrolle

1.3.1 Rechtevergabe Kundenbereich

Jeder Datensatz eines Testteilnehmers wird durch drei Felder kategorisiert:
a) Durch eine eindeutige Partner-ID ist festgelegt, zu welchem Auftraggeber ein Datensatz gehört. Durch diese Maßnahme ist sichergestellt, dass jeder Auftraggeber grundsätzlich nur auf die von ihm generierten Teilnehmerdatensätze Zugriff hat. Diese Zuordnung lässt sich durch keine Rechtevergabe oder Ähnliches übergehen.
b) Durch die Aktions-ID wird die Aktion, bzw. das Projekt festgelegt, in dessen Rahmen die Testteilnahme stattfindet. Für jede Aktion können individuelle Einstellungen, beispielsweise der Anonymisierungszeitraum, hinterlegt werden. Durch die gepedu bzw. die Masteraccounts des Auftraggebers wird festgelegt, auf welche Aktionen (dieses Auftraggebers) ein Account zugreifen kann.
c) Als drittes Feld legt die Bestell-ID fest, von welchem Mitarbeiter/Account eines Auftraggebers ein Zugangscode angefordert wurde. Jeder Standard-Account kann immer nur solche Daten verwalten, die über seinen Account generiert wurden. Nur Master-Accounts eines Auftraggebers können Account-übergreifende Daten (dieses Auftraggebers) einsehen.

1.3.2 Zugriffmöglichkeiten Kundenbereich

Im Kundenbereich können die Testungen (beispielsweise die Vergabe von Zusatzcodes, Check des Auswertungsdatums etc.) der Teilnehmer nachverfolgt und kontrolliert werden. Es gibt jedoch keine Möglichkeit, die Rohdaten aus den Online-Testungen einzusehen, zu kopieren, zu ändern oder zu löschen. Es können lediglich solche Rohdaten eingesehen werden, die vom Auftraggeber selbst (beispielsweise zur Ergänzung der Auswertung) eingegeben werden.

1.3.3 Verarbeitung der Daten durch die gepedu

Alle routinemäßigen und weitgehend automatisch durchgeführten Verarbeitungsschritte durch die gepedu werden protokolliert oder durch ein Ausführungsdatum dokumentiert. Dazu gehört auch die regelmäßige Verarbeitung von Anfragen der Teilnehmer, beispielsweise zu organisatorischen oder technischen Anfragen, sowie regelmäßig anfallende Verarbeitungsschritte wie beispielsweise das Markieren unzustellbarer E-Mailadressen.

1.3.4 Administration der Datenbanken durch die gepedu

Der administrative Zugriff auf die Daten der gepedu ist auf einen sehr kleinen, besonders geschulten Personenkreis beschränkt.

1.4 Trennungsgebot

Die auf dem Webserver erhobenen Teilnehmerdaten werden nach den schon unter Absatz 1.3.1 genannten Datenbankfeldern (Partner-ID, Aktions-ID und Bestell-ID) getrennt. Diese drei Felder sorgen im Kundenbereich für die strikte Trennung nach Kunden/Auftraggebern (Partner-ID), die zweckgerichtete Auswertung (Aktions-ID), sowie die Zuordnung zu den verantwortlichen Mitarbeiterinnen und Mitarbeitern des Auftraggebers (Bestell-ID). Die Zuordnung zu den verantwortlichen Mitarbeitern kann nur von Masteraccounts (für Mitarbeiter des Auftraggebers) übergangen werden, die dafür über die notwendigen Datenbankrechte verfügen.
Die gepedu verfügt zudem über gesonderte Testrechner für Entwicklungszwecke, um Produktiv- und Testsysteme zu trennen.

2. Maßnahmen zur Sicherung der Integrität

2.1. Weitergabekontrolle

2.1.1. Weitergabe von Daten an den Auftraggeber

Für alle vollständig bearbeiteten Testungen werden zeitnah die Auswertungsdokumente in PDF-Form erstellt. Dies geschieht in der Regel innerhalb von 24 Stunden und wird nur dann aufgeschoben, wenn beispielsweise bei einer Gruppentestung auf weitere Teilnehmer gewartet wird. Als Auswertung erhält der Auftraggeber in der Regel eine oder mehrere Auswertungsdokumente. Alle Auswertungsdokumente eines Auswertungslaufs werden als verschlüsselte Zip-Datei gespeichert und augenblicklich per E-Mail an die für den Auswertungsversand im Kundenbereich für den zugehörigen Account hinterlegte E-Mail-Adresse geschickt. Die Adresse für den Auswertungsversand kann vom Account des Auftraggebers selbst administriert werden (beispielsweise bei Urlaubsvertretung etc.). Das Passwort für die Verschlüsselung wird jedoch von der gepedu vorgegeben und kann vom Auftraggeber nicht geändert werden. So wird sichergestellt, dass eine nach derzeitigem technischem Stand ausreichende Passwortlänge und -komplexität verwendet wird (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen, keine Trivialpasswörter).
Die Entschlüsselung der Zip-Datei funktioniert nur bei vollständig intakten Dateien. Somit wird sichergestellt, dass es bei der Übermittlung der Daten nicht zu unbemerkten Übertragungsfehlern kommen kann. Durch die Wahl des plattformübergreifenden PDF-Formats wird zudem sichergestellt, dass die Auswertungsdokumente beim Empfänger richtig dargestellt werden.

Das Übergabedatum an den Auftraggeber wird als Auswertungsdatum bei jedem Datensatz gespeichert. Mit Erstellung der Auswertung der Auswertung wird gleichzeitig das Anonymisierungsdatum eingetragen. Bis zum Erreichen dieses Datums kann auf Anfragen des Auftraggebers reagiert werden, beispielsweise, wenn eine Auswertungs-E-Mail versehentlich gelöscht wurde. So wird sichergestellt, dass die Auswertungsdokumente für den Auftraggeber auch bei technischen Problemen bis zum Anonymisierungsdatum verfügbar bleiben.

Das Auswertungsdatum kann zusammen mit der zugehörigen Drucknummer im Kundenbereich eingesehen werden. Somit können die Übermittlungsvorgänge durch den Auftraggeber kontrolliert werden.

2.1.2. Interne Datenverarbeitung durch die gepedu

Bei Zugriffen auf Daten des Webservers durch die gepedu werden die unter Absatz 1.2.2 beschriebenen Maßnahmen verwendet (beispielsweise SSL-gesicherte Verbindungen/Tunnel). Bei Importen der Daten werden zusätzliche Kennwerte gebildet, um die Vollständigkeit der Daten überprüfen zu können. Der Import der Teilnehmerdaten wird zudem protokolliert. Ein unveränderter Referenzdatensatz bleibt zusätzlich auf dem Server zur Sicherstellung der Verfügbarkeit bis zum Erreichen des Anonymisierungsdatums bestehen.

2.2. Eingabekontrolle

2.2.1. Bearbeitung der Online-Fragebögen durch die Teilnehmer

Bei allen Online-basierten Testverfahren der gepedu werden sämtliche inhaltsbezogene Daten durch die Teilnehmerinnen und Teilnehmer selbst eingegeben. Diese Daten werden völlig automatisiert durch programm- und datenbankbasierte Verwaltungsdaten ergänzt (beispielsweise die Partner-ID zur Mandantenkennzeichnung).

Bei der Eingabe der inhaltsbezogenen Daten durch die Teilnehmer werden diese Daten auf Vollständigkeit und Sinnhaftigkeit geprüft (Datumsangaben müssen beispielsweise ein gültiges Datum darstellen). Zu jeder einzelnen Frage (bzw. Aufgabe) im Onlinetest wird dazu das erlaubte Antwortformat sowie die Angabe, ob die Beantwortung verpflichtend ist, hinterlegt. Eine Seite des Fragebogens kann erst abgeschlossen werden, wenn dort sämtliche Pflichtangaben bearbeitet wurden und die Antworten

ein gültiges Format ausweisen. Fehlende Antworten oder Antworten in einem ungültigen Format werden durch rote Schrift hervorgerufen und den Teilnehmern zur Korrektur bzw. Ergänzung vorgelegt.

Durch diese technischen Maßnahmen wird sichergestellt, dass alle auszuwertenden Datensätze in einem gültigen und vollständigen Format vorliegen. Es gibt dementsprechend bei der gepedu keine regelmäßig eingesetzten Funktionen auf Mitarbeiterebene zur Veränderung oder Löschung einzelner Rohdaten, da diese weder benötigt noch erwünscht sind.
Sofern es durch Gründe wie Programmfehlern, Browserinkompatibilitäten oder Abbrüchen der Onlineverbindung zu Korrekturen an den Daten kommt, werden diese ausschließlich durch die Datenbankadministratoren vorgenommen.

Die Teilnehmer haben bei der Bearbeitung der Fragebögen die Möglichkeit, innerhalb eines Fragenblocks vor- und zurückzugehen und so ihre Eingaben zu kontrollieren, und wenn gewünscht zu korrigieren. So können sie eventuelle Fehleingaben selber korrigieren. Nach Beendigung des Onlinetests ist kein erneuter Login durch die Teilnehmer mehr möglich und die Daten können somit von diesen nicht mehr verändert werden.

Der Auftraggeber sieht im Kundenbereich lediglich die von den Teilnehmern angegeben Namen, sofern keine anonyme Teilnahme vereinbart wurde. Eine Möglichkeit für den Auftraggeber, die Fragebogendaten der Teilnehmer einzusehen oder zu verändern, besteht nicht.

2.2.2. Eingabe von Daten durch den Auftraggeber

Die gepedu bietet den Auftraggebern Eingabemasken für die Daten handlungsorientierter Testverfahren an. Diese Eingabemasken sind über den Kundenbereich zu erreichen. Die dort eingegebenen Daten können vom Auftraggeber eingesehen und verändert werden, bis die entsprechenden Datensätze von der gepedu zur Auswertung eingelesen wurden. Nach der Auswertung durch die gepedu können die dort eingegeben Daten nicht mehr verändert werden. Auch diese Daten sind mit einer eindeutigen Partner-ID, Aktions-ID und Bestell-ID verknüpft.

2.3. Auftragskontrolle (Webserverhosting)

Der von der gepedu für das Hosting des Webservers beauftragte Provider wurde sorgfältig ausgewählt. Hauptauswahlkriterien waren eine einem Rechenzentrum entsprechende Sicherheits-Infrastruktur sowie ein physischer Standort in Deutschland.

Die gepedu nutzt beim Provider einen eigenen physischen Server, auf den sie volle Zugriffsrechte besitzt. Sämtliche auf dem Server befindliche Scripte und Protokolle können daher von der gepedu eingesehen werden. Die vom Provider durchgeführten Maßnahmen zur Datensicherung sind mit der gepedu abgestimmt.

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeit

3.1.1. Sicherung der Webserverdaten
Siehe Dokument „Domainfactory_TOM_V1.1.pdf“ bzw. in eine aktualisierte Version dieses Dokuments.

3.1.2. Sicherung gepedu
Die lokalen Daten der gepedu werden regelmäßig gesichert. Der genaue Ablauf der Datensicherung wird im Dokument „Anlage 5 - Datensicherungskonzept gepedu“ beschrieben.

3.1.3. Verfügbarkeit der Datenverarbeitungssysteme
Wichtige Endgeräte (insbesondere Auswertungsrechner) sind mehrfach vorhanden. Ein Reserverechner kann binnen Minuten in Betrieb genommen werden, so dass auch bei einem Totalausfall der Auswertungssysteme die üblichen Auswertungsintervalle problemlos eingehalten werden können.
Bei einem Hardware-Ausfall des Webservers wird vom Provider innerhalb von maximal 2 bis 3 Stunden (in der Regel deutlich schneller) ein Ersatzgerät in Betrieb genommen.

3.2. Belastbarkeit der Systeme
Sämtliche Systeme der gepedu zur Datenverarbeitung sind technisch hoch optimiert und lasten daher die technisch verfügbaren Kapazitäten nur zu einem Bruchteil aus. Daher können auch starke Auslastungsspitzen problemlos bewältigt werden.
Die Auslastung des Webservers kann laufend durch ein Monitoring-Tool kontrolliert werden. Eine Aufrüstung/Anpassung an mögliche zukünftige Auslastungssteigerungen ist jederzeit kurzfristig möglich.

4. Anonymisierung und Pseudonymisierung

4.1. Anonymisierung
Jeder Teilnehmerdatensatz ist durch eine Aktions-ID mit den für diese Aktion geltenden Einstellungen verknüpft (siehe hierzu Punkt 1.3.1.b). Dadurch wird sichergestellt, dass für jeden Datensatz immer eine gültige Anonymisierungsfrist hinterlegt ist. Diese beträgt im Normalfall maximal 42 Tage, kann aber projektspezifisch davon abweichen.

4.2. Pseudonymisierung
Sofern der Auftraggeber eine anonyme Anmeldung der Teilnehmerinnen und Teilnehmer an den Testverfahren wünscht, findet eine pseudonymisierte Übertragung der Testergebnisse statt. In diesem Fall können die Teilnehmer nur durch den bei der Anmeldung verwendeten Zugangscode den von der gepedu erstellten Auswertungen zugeordnet werden. Diese Zuordnung ist nur durch den Auftraggeber möglich, da nur dieser die nötigen Zuordnungslisten besitzt.