

Vereinbarung zur Auftragsverarbeitung

abgeschlossen zwischen

Musterschule

Straße

PLZ Ort

nachfolgend als „Auftraggeber“ oder „Verantwortlicher“ bezeichnet

und

Fox Education Services GmbH

Liechtensteinstraße 25/DG

1090 Wien

nachfolgend als „Auftragnehmer“ oder „Auftragsverarbeiter“ bezeichnet

Präambel

Die Firma Fox Education Services GmbH bietet IT-Dienstleistungen für Schulen an. Dafür wird mit der jeweiligen Schule als Auftraggeber und Fox als Auftragnehmer ein Hauptvertrag über die zu erbringenden Leistungen geschlossen

Der Auftragsverarbeiter betreut auf Grundlage des Hauptvertrages folgende Applikationen:
SchoolFox

und erbringt in diesem Zusammenhang folgende IT-Leistungen:

Sichere Eltern-Lehrer-Schüler-Kommunikation

Dabei verarbeitet der Auftragnehmer als Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers. Da die DSGVO vorsieht, dass eine solche Verarbeitung personenbezogener Daten im Auftrag eine vertragliche Grundlage erfordert, schließen die Vertragsparteien die vorliegende Vereinbarung:

Die vorliegende Vereinbarung stellt die vertragliche Basis für die Auftragsverarbeitung gemäß Artikel 28 DSGVO dar und regelt die Rechte und Pflichten der Vertragsparteien im Hinblick auf eine datenschutzkonforme Auftragsverarbeitung. Die vorliegende Vereinbarung

konkretisiert somit den zwischen dem Auftraggeber (als Verantwortlichen nach Artikel 4 Abs 7 DSGVO) und dem Auftragnehmer abgeschlossenen „Hauptvertrag“ bezüglich der Verarbeitung personenbezogener Daten durch den Auftragnehmer (als Auftragsverarbeiter nach Artikel 4 Abs 8 DSGVO) im Auftrag des Auftraggebers.

Die Kategorien der von der Datenverarbeitung betroffenen Personen lauten wie folgt:
PädagogInnen, Schulleitung, Eltern, SchülerInnen

Diese Auftragsverarbeitervereinbarung ist der jeweiligen Schule im Zuge des Abschluss des Hauptvertrages zwischen Schule und Fox Education Service GmbH zur Kenntnis zu bringen und wird von den Vertragsparteien des Hauptvertrags als integraler Vertragsbestandteil vereinbart.

Im Zuge der Leistungserbringung durch den Auftragnehmer unter dem Hauptvertrag verpflichtet sich der Auftragnehmer die folgenden datenschutzrechtlichen und datensicherheitstechnischen Bestimmungen einzuhalten:

1. Diese Vereinbarung tritt mit Beauftragung gemäß Hauptvertrag in Kraft und gilt für die gesamte Dauer der aufrechten Vertragsbeziehung zur Erbringung der Leistungen gemäß dem Hauptvertrag, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.
2. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er bei der Verarbeitung personenbezogener Daten alle anwendbaren Datenschutz- und Datensicherheitsbestimmungen, insbesondere jedoch nicht abschließend, die Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) einhält.
3. Bei Vorliegen der Voraussetzungen des Art 37 DSGVO ist der Auftragsverarbeiter (zumindest) für die Laufzeit dieser Vereinbarung verpflichtet, einen Datenschutzbeauftragten bestellen. Der Auftragsverarbeiter hat insbesondere sicherzustellen, dass der Datenschutzbeauftragte an allen Angelegenheiten, die den Datenschutz betreffen, ordnungsgemäß und frühzeitig beteiligt ist und dieser seinen Aufgaben gemäß Art 39 nachkommen kann. Der Auftragsverarbeiter teilt dem Auftraggeber die nach Art. 37 Abs. 7 DSGVO veröffentlichten Kontaktdaten des Datenschutzbeauftragten sowie den Link zur Veröffentlichung mit.
4. Der Auftragsverarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeiten für den Auftraggeber gemäß Art. 30 Abs. 2 DSGVO. Der Auftraggeber stellt dem

Auftragsverarbeiter auf Anfrage für diesen Zweck die relevanten Auszüge aus seinem Verzeichnis von Verarbeitungstätigkeiten in digitaler Form (PDF) zur Verfügung. Der Auftragsverarbeiter stellt sein Verzeichnis von Verarbeitungstätigkeiten auf Anfrage der Aufsichtsbehörde zur Verfügung (Art 30 Abs 4 DSGVO).

5. Pflichten, die sich nicht bereits aus dem Hauptvertrag oder dem objektiven Recht ergeben, hat der Auftraggeber durch gesonderte „Weisungen zur Datenverarbeitung“ in Anlage 2 auszudrücken, welche vom Auftragsverarbeiter einzuhalten sind. Der Auftraggeber kann alle Weisungen jederzeit durch eine entsprechende Mitteilung ändern oder ersetzen. Falls der Auftraggeber mündlich spezifische Weisungen zur Datenverarbeitung erteilt, müssen diese anschließend in Textform (z.B. per E-Mail) bestätigt werden.
6. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person dürfen Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der dokumentierten Aufträge und Weisungen des Auftraggebers verarbeiten und übermitteln, außer es liegt ein Ausnahmefall gemäß Art 28 Abs 3 lit a DSGVO (gesetzliche Verpflichtung des Auftragsverarbeiters) vor. Im letzteren Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs 3 letzter Satz DSGVO).
7. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des Art. 28 Abs. 3 lit. b DSGVO und § 6 österreichisches Datenschutzgesetz nachweislich verpflichtet hat und diese auf die verwaltungsstrafrechtlichen Konsequenzen eines Verstoßes hingewiesen worden sind. Kopien dieser Verpflichtungserklärungen sind auf formloses Ersuchen unverzüglich dem Auftraggeber zu übermitteln. Insbesondere bleibt die Verschwiegenheitsverpflichtung des Auftragsverarbeiters und der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Der Auftragsverarbeiter ist zudem verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen sowie Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

8. Alle dem Auftragsverarbeiter unterstellten Personen, die mit der Verarbeitung personenbezogener Daten im Verantwortungsbereich des Auftraggebers betraut sind, müssen im Hinblick auf Datenschutz, Datensicherheit und Vertraulichkeit angemessen geschult sein. Der Auftragsverarbeiter hat die erforderlichen Schritte zu unternehmen, um sicherzustellen, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese nur gemäß den Weisungen des Auftraggebers verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet (Art 32 Abs 4 DSGVO).
9. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO ergriffen hat, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu erreichen und um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Zum Beleg der Einhaltung von technischen und organisatorischen Maßnahmen können vorhandene, gültige Zertifizierungen nach ISO 27000, ISO 29134, BSI-Grundschutz, CNIL oder ähnliche dienen, die dem Auftraggeber vor Unterzeichnung der vorliegenden Vereinbarung vorzulegen und welche als Anlage der Vereinbarung anzuschließen sind. Bei Fehlen entsprechender Zertifikate und Testate sind ausführliche Dokumentationen der getroffenen technischen und organisatorischen Maßnahmen vorzulegen und als Anlage dieser Vereinbarung anzuschließen, welche die Einhaltung eines dem Risiko angemessenen Schutzniveaus belegen.
10. Der Auftragsverarbeiter darf ein anderes Unternehmen als weiteren Auftragsverarbeiter nach Art. 4 Abs. 8 DSGVO nur dann heranziehen, wenn der Auftraggeber dem schriftlich zustimmt (Art. 28 Abs. 2 DSGVO). Der Auftragsverarbeiter muss mit dem Sub-Auftragsverarbeiter einen Vertrag im Sinne des Art. 28 Abs. 4 DSGVO abschließen. In diesem Vertrag hat der Auftragsverarbeiter sicherzustellen, dass der Sub-Auftragsverarbeiter nachweislich dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund der DSGVO, dem DSG sowie dieser Vereinbarung und der zugrunde liegenden Beauftragung obliegen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Bestimmungen erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters (Art 28 Abs. 4 letzter Satz DSGVO).

11. Der Auftragsverarbeiter hat dem Auftraggeber unverzüglich alle erforderlichen Informationen zum Nachweis der Einhaltung seiner rechtlichen (insbesondere gem. DSGVO und DSG) und vertraglichen Pflichten zur Verfügung zu stellen. Der Auftragsverarbeiter trägt insbesondere für die technischen und organisatorischen Voraussetzungen Sorge, dass der Auftraggeber die Rechte betroffener Personen gemäß Art 12 bis 23 DSGVO (Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung etc.) gegenüber den betroffenen Personen innerhalb der gesetzlichen Fristen rechtskonform erfüllen kann. Für den Fall, dass sich eine betroffene Person direkt an den Auftragsverarbeiter zwecks Geltendmachung seiner Rechte wenden sollte, hat der Auftragsverarbeiter ihr Begehren unverzüglich an den Auftraggeber weiterzuleiten. Dem Auftragsverarbeiter ist es untersagt, der betroffenen Person nähere Informationen über die Datenverarbeitung des Auftraggebers zu erteilen, ausgenommen davon ist die Nennung des Namens und der Kontaktdaten des Auftraggebers.
12. Der Auftragsverarbeiter ist gemäß Art. 28 Abs. 3 lit. g DSGVO nach Beendigung der Verarbeitungsleistungen verpflichtet, nach Wahl des Auftraggebers alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder (nach vorheriger Zustimmung des Auftraggebers) zu vernichten, sofern nicht nach dem Unionsrecht oder dem für den Auftragsverarbeiter geltenden nationalen Recht eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung (Vernichtung) ist auf Anforderung dem Auftraggeber unverzüglich vorzulegen. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung seiner Verarbeitungsleistungen entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten erhalten hat oder in einem anderen, gängigen Format (für den Auftraggeber kostenfrei) herauszugeben.
13. Der Auftragsverarbeiter verpflichtet sich, bei der elektronischen Übermittlung von Daten technische Verfahren mit Authentifikation und Verschlüsselung nach den üblichen Sicherheitsstandards unter besonderer Berücksichtigung der Vorgaben nach Art. 32 DSGVO anzuwenden.
14. Sollte für die Auftragsverarbeitung eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO nötig sein, verpflichtet sich der Auftragsverarbeiter dem Auftraggeber alle für die Erstellung der DSFA erforderlichen Informationen zeitgerecht zur Verfügung zu stellen. Der Auftragsverarbeiter verpflichtet sich, den

Auftraggeber bei der Einhaltung der übrigen in den Art 32, 33, 34 und 36 DSGVO genannten Pflichten zu unterstützen und dem Auftraggeber dafür alle erforderlichen Informationen unverzüglich zu übermitteln.

15. Der Auftragsverarbeiter setzt geeignete technische und organisatorische Maßnahmen um, die sicherstellen, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt. Der Auftragsverarbeiter ist verpflichtet dem Auftraggeber einen entsprechenden Nachweis gemäß Art. 24 Abs. 1 vor Beginn der Verarbeitungstätigkeit zur Verfügung zu stellen.
16. Der Auftragsverarbeiter verpflichtet sich, geeignete technische und organisatorische Maßnahmen, wie Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellungen zu treffen, sowie Garantien in die Verarbeitung mitaufzunehmen, die sicherstellen, dass die Vorgaben des Art. 25 DSGVO eingehalten werden.
17. Der Auftragsverarbeiter übermittelt dem Auftraggeber vor Beginn der Verarbeitungstätigkeit alle Nachweise über eingehaltene Verhaltensregeln nach Art. 40 DSGVO, sowie erlangte Zertifikate nach Art. 42 DSGVO, welche die beauftragte Verarbeitungstätigkeit betreffen, zur Erstellung der Risikoabschätzung gemäß Art. 32 Abs. 1 DSGVO.
18. Für die IT-Systeme des Auftragsverarbeiters sind weiters die einschlägigen Vorgaben des Österreichischen Informationssicherheitshandbuches in der geltenden Fassung anzuwenden. So die Daten nicht auf der vom Auftraggeber bereitgestellten Server-Infrastruktur gehostet werden, ist nachzuweisen, dass die für den Betrieb herangezogenen Server-Infrastruktur jedenfalls eine gültige Zertifizierung nach ISO 27001 oder gleichwertig besitzen.
19. Der Auftragsverarbeiter verpflichtet sich, Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 oder Art. 34 DSGVO unverzüglich schriftlich an den Auftraggeber, sowie per E-Mail an den Datenschutzbeauftragten des Auftraggebers unter <E-Mail> zu melden.
20. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz, die Einhaltung der zwischen den Vertragsparteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren bzw. durch im Einzelfall zu benennende, sachverständige Dritte (mit oder ohne Beisein des Auftraggebers) kontrollieren zu lassen. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen nach Art. 28 Abs. 3 lit. h DSGVO eingeräumt. Der Auftraggeber kann dazu die Kontrolle in der

Betriebsstätte des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen bzw. vornehmen lassen.

21. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber unverzüglich von jedem Verstoß des Auftragsverarbeiters, seiner betrauten Mitarbeiter oder Dritter gegen anwendbare Datenschutzvorschriften oder in dieser Vereinbarung getroffene Pflichten und Weisungen in Kenntnis zu setzen. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
22. Der Auftragsverarbeiter ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber gemäß Art 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende (geplante) Maßnahmen vom Auftragsverarbeiter zu informieren.
23. Der Auftragsverarbeiter verpflichtet sich, die Datenverarbeitung in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Dies gilt insbesondere für Hosting, jedoch nicht unbedingt für Call Center, IT Wartung, Rechnungserstellung und sonstige administrative Services, die gegebenenfalls auch in einem Drittland erbracht werden. Jedwede, sei es auch nur eine teilweise, Erbringung der Datenverarbeitung in einem Drittland bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers. Sofern der Auftraggeber einer Erbringung der Datenverarbeitung in einem Drittland zugestimmt hat, darf diese nur dann erfolgen, wenn alle gesetzlichen und vertraglichen Voraussetzungen nachweislich erfüllt sind.
24. Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren.
25. Die Vertragsparteien schließen die Anwendung etwaiger im Hauptvertrag enthaltener Haftungsprivilegierungen bzw. -beschränkungen zugunsten des Auftragsverarbeiters auf datenschutzrechtliche Verstöße ausdrücklich aus.
26. Änderungen und Ergänzungen zu diesem Vertrag bedürfen der Schriftform. Gleiches gilt für die Vereinbarung, vom Erfordernis der Schriftform abzugehen. Die dieser Vereinbarung beigefügten Anhänge bilden einen integrierenden Vertragsbestandteil.

27. Diese Vereinbarung unterliegt dem österreichischen Recht sowie dem sachlich anwendbaren Unionsrecht. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung ist Wien, Österreich.

28. Diese Vereinbarung wird in zwei (2) Originalen ausgefertigt, von welchen jede Vertragspartei ein Original erhält.

Für den Auftraggeber:

Für den Auftragnehmer:

Unterschrift:

Unterschrift:

Name:

Name:

Funktion:

Funktion:

Datum:

Datum:

ANLAGEN

Anlage 1

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Für geringen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit gem. Art 32. Sollte höherer Schutzbedarf vorliegen ist zusätzlich zu dieser Anlage gemeinsam mit dem Vertreter des Verantwortlichen eine ausführliche Risikoanalyse durchzuführen. Zur Einschätzung des Schutzbedarfs siehe:

<http://pubshop.bmbf.gv.at/ergebnis.aspx?s=datenschutz&t=00>

Führen Sie im Folgenden die jeweils getroffenen technischen und organisatorischen Maßnahmen gemäß dieser Tabelle an:

1.	Fähigkeit der Vertraulichkeit Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	<input checked="" type="checkbox"/> Elektronisches Zutrittskontrollsystem <input checked="" type="checkbox"/> Sicherheitstüren und/oder -fenster <input type="checkbox"/> Gitter vor Fenstern und Türen <input checked="" type="checkbox"/> Werkschutz, Pfortner <input checked="" type="checkbox"/> Alarmanlage <input checked="" type="checkbox"/> Videoüberwachung <input checked="" type="checkbox"/> Spezielle Schutzvorkehrungen für den Serverraum <input checked="" type="checkbox"/> Individueller Log-In und Kennwortverfahren <input checked="" type="checkbox"/> Zusätzlicher Log-In für bestimmte Anwendungen <input type="checkbox"/> Automatische Sperrung der Clients (Zeitablauf) <input checked="" type="checkbox"/> Verwaltung von Berechtigungen <input checked="" type="checkbox"/> Dokumentation von Berechtigungen <input checked="" type="checkbox"/> Verschlüsselung von Systemen <input checked="" type="checkbox"/> Verschlüsselung der Kommunikation <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern <input type="checkbox"/> VPN (Virtual Private Network) <input checked="" type="checkbox"/> Gesichertes WLAN <input checked="" type="checkbox"/> SSL-Verschlüsselung bei Web-Access <input type="checkbox"/> Sonstige:
----	--	---

2.	<p>Fähigkeit der Integrität</p> <p>Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet?</p> <p>Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.</p>	<input checked="" type="checkbox"/> Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern <input checked="" type="checkbox"/> Verwendung von Zugriffsrechten <input checked="" type="checkbox"/> Systemseitige Protokollierungen <input checked="" type="checkbox"/> Funktionelle Verantwortlichkeiten <input type="checkbox"/> Sonstige:
3.	<p>Fähigkeit der Verfügbarkeit</p> <p>Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet?</p> <p>Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.</p>	<input checked="" type="checkbox"/> Back-Up Verfahren <input type="checkbox"/> Spiegeln von Festplatten <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) <input checked="" type="checkbox"/> Virenschutz /Firewall <input checked="" type="checkbox"/> Notfallplan <input type="checkbox"/> Klimaanlage <input checked="" type="checkbox"/> Brand- und Löschwasserschutz <input checked="" type="checkbox"/> Alarmanlage <input type="checkbox"/> Geeignete Archivierungsräumlichkeiten <input type="checkbox"/> Sonstige:
4.	<p>Fähigkeit der Belastbarkeit</p> <p>Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet?</p> <p>Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.</p>	<input checked="" type="checkbox"/> Penetrationstests <input checked="" type="checkbox"/> Lasttests <input type="checkbox"/> Sonstige:
5.	<p>Wiederherstellbarkeit der Verfügbarkeit und des Zugangs</p> <p>Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?</p>	<input checked="" type="checkbox"/> Back-Up Verfahren <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) <input checked="" type="checkbox"/> Notfallplan <input type="checkbox"/> Vertretungsregelungen <input type="checkbox"/> Sonstige:

6.	<p>Pseudonymisierung</p> <p>Wie wird die Pseudonymisierung der Daten gewährleistet?</p> <p>Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.</p>	<input type="checkbox"/> Personenbezogene Daten werden durch Zufallscodes ersetzt <input type="checkbox"/> Data Masking <input checked="" type="checkbox"/> Sonstige: Die Datenverarbeitung erfolgt pseudonymisiert, sodass Datensätze nicht ohne weitere Informationen einer Person zugeordnet werden können. Diese Informationen werden separat gespeichert.
7.	<p>Verschlüsselung</p> <p>Wie wird die Verschlüsselung gewährleistet?</p> <p>Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext (Chiffre), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.</p>	<input type="checkbox"/> Nutzung von kryptografischen Tools <input type="checkbox"/> Data Hashing <input checked="" type="checkbox"/> Verschlüsselung von Speichermedien <input checked="" type="checkbox"/> Verschlüsselung der Kommunikation <input type="checkbox"/> Sonstige:
8.	<p>Verfahren zur regelmäßigen Überprüfung*</p> <p>Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?</p>	<input checked="" type="checkbox"/> Es existiert eine festgelegte Prüfroutine <input type="checkbox"/> Prüfberichte werden evaluiert <input type="checkbox"/> Implementierung von Verbesserungsvorschlägen <input type="checkbox"/> Sonstige:
9.	<p>Unrechtmäßiger Zugang zu personenbezogenen Daten</p> <p>Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?</p>	<input checked="" type="checkbox"/> Individueller Log-In und Kennwortverfahren <input checked="" type="checkbox"/> Zusätzlicher Log-In für bestimmte Anwendungen <input type="checkbox"/> Automatische Sperrung der Clients (Zeitablauf) <input checked="" type="checkbox"/> Verwaltung von Berechtigungen <input checked="" type="checkbox"/> Dokumentation von Berechtigungen <input type="checkbox"/> Verschlüsselung von Systemen <input type="checkbox"/> Sonstige:

10.	<p>Verarbeitung personenbezogener Daten nur nach Anweisung</p> <p>Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?</p>	<p><input checked="" type="checkbox"/> Mitarbeiter sind zu Verhaltensregeln verpflichtet</p> <p><input checked="" type="checkbox"/> Implementierung unternehmensinterner Datenschutz-Richtlinien</p> <p><input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter auf das Datengeheimnis</p> <p><input checked="" type="checkbox"/> Schulungen aller zugriffsberechtigten Mitarbeiter</p> <p><input checked="" type="checkbox"/> Bestimmung von Ansprechpartnern für den konkreten Auftrag</p> <p><input type="checkbox"/> Sonstige:</p>
-----	--	--

Anlage 2

***(allfällige) Weisungen zur Datenverarbeitung,
soweit zusätzlich zum Hauptvertrag erforderlich***