AUFTRAGSVERARBEITUNG

Dieser Vertrag regelt die datenschutzrechtlichen Pflichten des Kunden und der

Deubner Verlag GmbH & Co. KG, Oststraße 11, 50996 Köln (Auftragnehmer - Deubner)

in Bezug auf die Auftragsverarbeitung im Rahmen der Nutzung von Homepage-Services und sonstigen Produkten, in denen personenbezogene Daten verarbeitet werden.

1. Der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen ergeben sich aus dem Hauptvertrag zwischen den Parteien. Der Auftrag endet mit Beendigung des Hauptvertrages und Erfüllung der Pflichten nach Ziffer 9.

2. Deubner hält in seinem Verantwortungsbereich die vereinbarten technischen und organisatorischen Maßnahmen gemäß Art.5 Abs. 1 und Art. 32 DSGVO ein und hat seine innerbetriebliche Organisation gemäß datenschutzrechtlichen Anforderungen gestaltet. Dies beinhaltet die in der Anlage dargestellten technisch organisatorischen Maßnahmen.

3. Eine Berichtigung, Sperrung oder Löschung der im Auftrag verarbeiteten Daten nimmt Deubner nur nach Weisung des AG vor. Ist der AG aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt AG hat Deubner hierzu schriftlich aufgefordert.

4. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen oder zu löschen oder die Verarbeitung einzuschränken. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder der Einschränkung der Verarbeitung wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Der Auftragnehmer wird den Auftraggeber im Falle der Geltendmachung gesetzlicher Betroffenenrechte unterstützen; dies umfasst insbesondere die Unterstützung bei der Beantwortung von Anträgen auf Wahrung der Betroffenenrechte mittels geeigneter technisch-organisatorischer Maßnahmen.

5. Der Auftragnehmer gewährleistet die Einhaltung der folgenden Pflichten:

a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Sofern ein Wechsel in der Person des Datenschutzbeauftragten stattfindet, wird dies dem Auftraggeber unverzüglich mitgeteilt.

b) Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen schriftlich zur Vertraulichkeit verpflichtet sein und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Auf Anfrage des Auftraggebers wird der Auftragnehmer diesem die Verpflichtungserklärungen vorlegen. Dies ist nicht notwendig, soweit für die betreffenden Personen eine angemessene gesetzliche Verschwiegenheitspflicht besteht.

c) Duldung öffentlicher Kontrollen durch die zuständigen Datenschutzaufsichtsbehörden in gleichem Umfang, wie die Datenschutzaufsichtsbehörden Prüfungen beim Auftraggeber durchführen dürfen. Unterstützung des Auftraggebers bei Kontrollen und Anfragen der Aufsichtsbehörden.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde nach Art. 82 ff. DSGVO bei dem Auftragnehmer ermittelt.

e) Die angemessene Unterstützung des Auftraggebers bei der Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 DSGVO.

f) Die angemessene Unterstützung des Auftraggebers bei Datenschutz-Folgenabschätzungen gem. Art. 35 DSGVO und bei der vorherigen Konsultation der zuständigen Datenschutzaufsichtsbehörden nach Art. 36 DSGVO.

g) Die angemessene Unterstützung des Auftraggebers bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) und bei der Benachrichtigung der von Verletzungen des Schutzes personenbezogener Daten betroffenen Personen (Art. 34 DSGVO).

h) Die Vorlage der nach Art. 30 Abs. 2 DSGVO erforderlichen Angaben.

6. AG ist damit einverstanden, dass Deubner zur Erfüllung seiner vertraglichen Leistungen verbundenen Unternehmen Unteraufträge erteilt. Bei Erteilung eines Unterauftrags werden die vertraglichen Vereinbarungen zwischen Deubner und dem Unterauftragnehmer so gestaltet, dass sie den Anforderungen zu Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. AG kann bei nachgewiesenen berechtigten Interessen einer Unterbeauftragung widersprechen. Deubner erteilt AG auf dessen schriftliche Aufforderung hin Auskunft über den wesentlichen Vertragsinhalt (Leistungen ausschließlich Preise) und die Umsetzung der datenschutzrelevanten Pflichten des Unterauftragnehmers.

7. Die Verarbeitung der Daten durch den Auftragnehmer ist räumlich auf die EU und den EWR beschränkt. Die Übermittlung von Daten durch den Auftragnehmer an einen Empfänger mit Sitz außerhalb des EWR ist nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig und bedarf der gesonderten vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer wird insbesondere sicherstellen, dass der Auftraggeber die Standardvertragsklauseln (vgl. z.B. die Entscheidung der Europäischen Kommission vom 5. Februar 2010, veröffentlicht im Amtsblatt der Europäischen Union L39/5, C (2010) 593) mit dem Empfänger der Daten abschließen kann.

8. AG kann sich nach rechtzeitiger schriftlicher Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Gesetze über den Datenschutz überzeugen. Deubner ist verpflichtet, die Kontrollen des AG nach diesem Vertrag zu dulden,

Mitwirkungsleistungen zu erbringen, soweit für die Kontrolle des AG nach diesem Vertrag erforderlich, und dem AG auf schriftliche Anforderung innerhalb einer angemessenen Frist Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind. Deubner ermöglicht dem AG insbesondere, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

9. Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber unverzüglich nach Kenntniserlangung eine Meldung, wenn durch ihn, die bei ihm beschäftigten Personen oder die von ihm eingesetzten Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz der Daten des Auftraggebers (insbesondere die DSGVO) oder gegen die in dieser Vereinbarung getroffenen Festlegungen vorgefallen sind bzw. ein entsprechender Verdacht besteht. Der Auftragnehmer wird entsprechende Vorfälle dokumentieren, unverzüglich aufklären und Abhilfe schaffen. Er wird den Auftraggeber über den Fortgang der Angelegenheit bis zur Behebung des Vorfalls informiert halten. Sollte die Verletzung zu einem Risiko für die Rechte und Freiheiten der Betroffenen gem. Art. 33 DSGVO führen, wird der Auftragnehmer den Auftraggeber bei der Aufklärung des Vorfalls und im Rahmen der entsprechenden Meldung an die Datenschutzaufsichtsbehörde bzw. die Betroffenen umfassend unterstützen.

10. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer wird die Weisungen soweit erforderlich dokumentieren.

11. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und lediglich für diese Zwecke zu nutzen. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Deubner unterrichtet AG unverzüglich bei Verstößen von Deubner oder der dort beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, auch bei schwerwiegenden Störungen des Betriebsablaufes oder bei Verdacht auf Datenschutzverletzungen.

13. AG ist nach freiem Ermessen zur Erteilung von Weisungen an Deubner in Bezug auf die Datenverarbeitung berechtigt. Deubner darf Daten nur im Rahmen des Vertrages und der Weisungen des AG erheben, verarbeiten oder nutzen. Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Berichtigung, Sperrung, Löschung, Herausgabe) von Deubner mit personenbezogenen Daten gerichtete schriftliche Anordnung des AG. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Ist Deubner der Ansicht, dass eine Weisung des AG gegen Vorschriften über den Datenschutz verstößt, hat er AG unverzüglich darauf hinzuweisen. Erteilt AG Einzelweisungen, die über die Anforderungen der DSGVO und des BDSG oder über die Anforderungen von anderen datenschutzrechtlichen Gesetzen hinausgehen, trägt AG sämtliche Deubner dadurch verursachten Kosten.

14. Vorbehaltlich abweichender Vereinbarungen und gesetzlicher oder satzungsmäßiger Pflichten ist Deubner nach Vertragsende verpflichtet, ihm überlassene Datenträger an AG unverzüglich zurück zu geben und ihm in Zusammenhang mit dem Auftrag übergebene und noch nicht gelöschte personenbezogene Daten zu löschen. Über die Herausgabe oder Löschung nach Vertragsende muss AG innerhalb einer von Deubner gesetzten Frist entscheiden. Wenn Deubner zu vernichtende Unterlagen oder Datenträger mit personenbezogenen Daten dem AG nicht zurückgibt, so ist Deubner verpflichtet, die Unterlagen ordnungsgemäß zu entsorgen, ohne dass unbefugte Dritte von den Daten Kenntnis erlangen können. Entstehen Deubner nach Vertragsbeendigung Kosten durch die Herausgabe oder Löschung der Daten des AG, so trägt diese der AG.

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO, § 64 BDSG)

1) Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
2) Diese Maßnahmen können unter anderem die Pseudonymisierung und die Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.
3) Die Maßnahmen sollen dazu führen, dass
a) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und,
b) dass die Verfügbarkeit personenbezogener Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.
4) Der Auftragsverarbeiter hat nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

Zugangskontrolle
- ✓ Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Zutrittskontrollsystem, zentrale Schlüsselverwaltung, Magnetkarte
- ✓ Schlüssel/Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- ✓ Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)
- ✓ Gebäudeschutz an Wochenenden und nachts gewährleistet
- ✓ Pförtner/Empfang mit Videoüberwachung
- ✓ Regelungen für Besucher (Besucherausweis, Begleitung im Gebäude)
- ✓ Videoüberwachung sensibler Bereiche des Gebäudes (Tiefgarage)
- ✓ Verschließen von Schränken und Büros bei Nichtanwesenheit

Datenträgerkontrolle
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Dezidiertes Kennwortverfahren zum Login [z.B. Klare Passwortregelung (bestimmte Länge, Kombination aus Buchstaben und Zahlen, keine Trivialpasswörter, Änderung in regelmäßigen Abständen). Voreingestellte Passwörter müssen umgehend geändert werden]
- ✓ Automatische Sperrung (z.B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität (ca. 5 min) mit anschließendem erneutem Login)
- ✓
- ✓ Automatischer Standby-Betrieb der lokalen Rechner
- ✓ Verschlüsselung von Datenträgern möglich
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträgern/Smartphones aus den Büroräumen heraus
- ✓ Möglichkeit der Fernlöschung von Smartphones

Speicherkontrolle
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Benutzerkontrolle
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Zugriffskontrolle
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Differenzierte Berechtigungen (Profile, Rollen)
- ✓ Differenziertes Ordnerkonzept (z.B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können).
- ✓ Datenträger sind eindeutig zu kennzeichnen und sicher aufzubewahren.
- ✓ Sichere Löschung von Daten und/ oder Vernichtung von Datenträgern.
- ✓ Ordnung am Arbeitsplatz [Datenträger (USB-Sticks, CD-ROMs) mit vertraulichem Material dürfen nicht offen herumliegen].
- ✓ Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen
- ✓ Deinstallation bzw. Deaktivierung nicht benötigter sicherheitsrelevanter Programme und Funktionen (v.a. bei Smartphones)

Übertragungskontrolle
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Eingabekontrolle
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Protokollierungs- und Protokollauswertungssysteme werden eingesetzt bzw. sind als Teile von bestehenden Softwareapplikationen anwendbar
- ✓ Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- ✓ Keine Weitergabe von Passwörtern
- ✓ Zusätzlich zur automatischen Sperrung: manuelle Abmeldung beim Verlassen des Büros

Transportkontrolle
Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Verschlüsselung (insbes. Laptops)
- ✓ Tunnelverbindung (VPN = Virtual Private Network)
- ✓ Elektronische Signatur möglich
- ✓ Keine Benutzung von nicht freigegebener Hard-/ Software
- ✓ Keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern
- ✓ Vorsicht beim Umgang mit Backup-Bändern
- ✓ Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Zugriff auf Ausdrucke bekommt).
- ✓ Regelung zum Einsatz von USB-Sticks und CD-ROMs

Wiederherstellbarkeit
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Zuverlässigkeit
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Datenintegrität
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Auftragskontrolle
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Eindeutige Vertragsgestaltung/Standardvertrag zu Art. 28 DSGVO vorhanden
- ✓ Formalisierte Auftragserteilung (Auftragsformular)
- ✓ Kriterien zur Auswahl des Auftragnehmers wird stringent eingehalten
- ✓ Kontrolle der Vertragsausführung wird durch den DSB gewährleistet

Verfügbarkeitskontrolle
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Regelmäßiges Backup-Verfahren ist sichergestellt (Definition: Welche Daten werden wie lange gesichert?; Einbeziehung von Laptops und nicht vernetzten Systemen; Regelmäßige Kontrolle der Sicherungsbänder; Dokumentierung der Sicherungsverfahren)
- ✓ Getrennte Aufbewahrung von Daten ist gewährleistet
- ✓ Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- ✓ Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall im Serverraum
- ✓ Notfallplan besteht und wird regelmäßig geübt
- ✓ Notstromversorgung/Unterbrechungsfreie Stromversorgung (USV)
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträger aus den Büroräumen heraus
- ✓ Vertretungsregelungen, v.a. bzgl. Administrator

Trennbarkeit
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (Mandantenfähigkeit)
- ✓ Funktionstrennung, insbesondere zwischen Produktions- und Testdaten

Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen

- ✓ Regelmäßige fachliche Fortbildung der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten
- ✓ Schulung der Mitarbeiter im Umgang mit der IT und zur Schärfung des IT-Sicherheitsbewusstseins
- ✓ Sicherheitshinweise werden allen Mitarbeitern in geeigneter Form bekannt gegeben und sind dauerhaft abrufbar (z.B. durch Veröffentlichung im Intranet)
- ✓ Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- ✓ Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- ✓ Regelmäßige Prüfung der Effektivität der bestehenden technischen und organisatorischen Maßnahmen und Prüfung, ob neue technische und organisatorische Maßnahmen erforderlich sind (beides unter Hinzuziehung des Datenschutzbeauftragten)
- ✓ Regelmäßige und anlassbezogene Kontrolle der Funktionalität der IT, einschließlich unter dem Aspekt der Zutrittskontrolle
- ✓ Eskalations- und Meldewege bei sicherheitsrelevanten Vorkommnissen
- ✓ Verfügbarkeit der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten als Ansprechpartner bei allen Fragen zur IT-Nutzung und -sicherheit.