Auftragsverarbeitungsvereinbarung (AVV)

Stand: April 2026

1. Gegenstand des Vertrags

(a) Geltung: Diese Auftragsverarbeitungsvereinbarung (**AV-Vertrag**) ergänzt die Dienstleistungsvereinbarung zwischen dem Kunden (**Auftraggeber**) und dem Leistungserbringer (**Auftragnehmer**), soweit eine Dienstleistungsvereinbarung einschliesslich anwendbarer allgemeiner Geschäftsbedingungen (der **Vertrag**) auf diesen AV-Vertrag verweist und der Auftragnehmer personenbezogene Daten des Auftraggebers (die **Auftragsdaten**) in Erfüllung des Vertrags verarbeitet und unter Vorbehalt einer separat für die betreffenden Dienstleistungen abgeschlossenen Auftragsverarbeitungsvereinbarung. Der Auftragnehmer ist eine Gesellschaft der BKW-Gruppe; ein Verzeichnis der Gruppenmitglieder ist unter www.bkw.ch/de/ueber-uns/die-bkw-gruppe/unser-firmennetzwerk einsehbar.

(b) Der AV-Vertrag gilt zwischen dem Auftragnehmer und andererseits dem Auftraggeber und ggf. allen weiteren mit dem Auftraggeber in einer Gruppe verbundenen Gesellschaften, die unter dem Vertrag zum Empfang von Leistungen berechtigt sind, bei deren Erbringung der Auftragnehmer Auftragsdaten verarbeitet. Soweit der Auftraggeber seinerseits als Auftragsverarbeiter eines anderen Verantwortlichen tätig ist, handelt der Auftragnehmer als Unterauftragnehmer. In diesem Fall gelten die Bestimmungen dieser AV-Vertrag als Unterauftragsverarbeitungsvereinbarung und sichert der Auftraggeber zu, dass die von ihm erteilten Weisungen den Weisungen des Verantwortlichen entsprechen.

(c) Gegenstand: Die Parteien regeln in diesem AV-Vertrag die Anforderungen an den Auftragnehmer im Zusammenhang mit der Verarbeitung der Auftragsdaten durch den Auftragnehmer. Die Dauer der Auftragsverarbeitung, ihre Art und ihr Zweck, die Kategorien der verarbeiteten Daten und die Kategorien betroffener Personen ergeben sich aus dem Vertrag. Im Fall eines Widerspruchs zwischen dem Vertrag und diesem AV-Vertrag gehen unter Vorbehalt von Ziff. 8(a) die zum Schutz der Personendaten strengeren Vorschriften vor.

(d) Definitionen: Fettgedruckte Begriffe werden in diesem AV-Vertrag jeweils mit der ihnen zugewiesenen Bedeutung verwendet. Rechtsbegriffe wie „Personendaten“, „Verarbeitung“, „Datensicherheitsverletzung“ usw. haben die im anwendbaren Datenschutzrecht festgelegte Bedeutung. Das **anwendbare Datenschutzrecht** meint das Schweizerische Bundesgesetz über den Datenschutz (**DSG**) und die zugehörige Verordnung, die Datenschutz-Grundverordnung (**DSGVO**) und andere datenschutzrechtliche Regelungen, jeweils soweit sie auf die Verarbeitung von Auftragsdaten zur Anwendung kommen. Verweisungen in diesem AV-Vertrag auf Bestimmungen des DSG bzw. der DSGVO sind als Verweisungen entsprechender Bestimmungen des jeweils anwendbaren Datenschutzrechts zu lesen.

(e) Dauer: Dieser AV-Vertrag gilt mit dem Abschluss des Vertrags, spätestens aber mit dem ersten Zugriff des Auftragnehmers auf Auftragsdaten, und endet mit Beendigung des Vertrags, frühestens aber mit der Löschung sämtlicher durch den Auftragnehmer verarbeiteten Auftragsdaten.

2. Allgemeine Pflichten des Auftragnehmers

(a) Befolgung von Weisungen:

(i) Der Auftragnehmer ist verpflichtet, Auftragsdaten ausschliesslich für die Erfüllung des Vertrags, dieses AV-Vertrags und der Weisungen des Auftraggebers zu verarbeiten. Vorbehalten sind abweichende Pflichten des anwendbaren zwingenden Rechts, über die der Auftraggeber soweit zulässig vorgängig zu informieren ist.

(ii) Weisungen über die Verarbeitung von Personendaten durch den Auftragnehmer sind verbindlich, soweit sie die Vertragspflichten nicht erweitern. Sie werden grundsätzlich über eine direkte Interaktion mit den Systemen des Auftragnehmers (sofern technisch möglich) oder in Textform erteilt; in dringenden Fällen können sie auch mündlich erfolgen. Der Auftraggeber ist verpflichtet, Weisungen angemessen zu dokumentieren.

(b) Personal: Der Auftragnehmer trifft geeignete Massnahmen, um sicherzustellen, dass seine Mitarbeitenden und beigezogene Dritte, die Zugang zu zur Erbringung der Dienstleistungen verarbeiteten Auftragsdaten haben können, zuverlässig, vertrauenswürdig und für die ihnen übertragenen Aufgaben im sicheren Umgang mit Daten angemessen geschult sind und die Auftragsdaten ausschliesslich nach den Bestimmungen dieses AV-Vertrags verarbeitet.

(c) Ort der Datenverarbeitung: Die Datenverarbeitungen werden ausschliesslich an den Standorten des Auftragnehmers vorgenommen, vorbehältlich der Auslagerung an beigezogene Unterauftragnehmer nach den Bestimmungen gemäss Ziff. 6. Sofern der Auftragnehmer beabsichtigt, Personendaten in einen Staat zu übermitteln, der nicht über ein nach dem anwendbaren Datenschutzrecht angemessenes Schutzniveau verfügt, schliesst er für diese Datenübermittlung eine Vereinbarung, die die Übermittlung nach dem anwendbaren Datenschutzrecht erlaubt.

(d) Rückgabe- und Löschpflicht:

(i) Wenn der Auftragnehmer Auftragsdaten nicht mehr zur Erfüllung seiner Pflichten gegenüber dem Auftraggeber benötigt, sorgt er dafür, dass die betreffenden Auftragsdaten an den Auftraggeber zurückgegeben und/oder verbleibende Kopien gelöscht werden. Der Auftraggeber hat dem Auftragnehmer bei Beendigung des AV-Vertrags entsprechende Weisungen zu erteilen.

(ii) Vorbehalten ist jeweils eine längere Speicherung in üblichen Backup-Systemen bis zur nächsten ordentlichen Löschung, sofern diese Systeme mindestens nach den Vorgaben dieses AV-Vertrags gesichert sind und die gespeicherten Auftragsdaten ausschliesslich für Backupzwecke verwendet werden.

3. Allgemeine Pflichten des Auftraggebers

(a) Die Verantwortung für die Rechtmässigkeit der Datenverarbeitung liegt beim Auftraggeber.

(b) Der Auftraggeber sichert die Rechtmässigkeit der Übertragung der Datenverarbeitung auf den Auftragnehmer und dessen entsprechender Verarbeitung zu. Bei besonderen Anforderungen an die Verarbeitung (wie bspw. erhöhten Sicherheitsbedarf) ist der Auftragnehmer entsprechend zu informieren.

4. Daten- und Informationssicherheit

4.1. Allgemeine Pflichten

(a) Der Auftragnehmer verpflichtet sich, angemessene technische und organisatorische Massnahmen zu ergreifen, um die zur Erbringung der Leistung verarbeitenden Auftragsdaten vor unzulässiger Verarbeitung zu schützen, mindestens aber die Massnahmen gemäss Anhang 1 «Technische und organisatorische Massnahmen» (die **TOM**).

(b) Der Auftraggeber bestätigt die Angemessenheit der TOM unter Berücksichtigung des von ihm beurteilten Schutzbedarfs der Auftragsdaten. Der Auftragnehmer kann die TOM jederzeit anpassen. Änderungen, die das Sicherheitsniveau der Auftragsdaten beeinträchtigen, sind dem Auftraggeber vorab in Textform mitzuteilen. Der Auftraggeber kann solchen Änderungen innerhalb einer Frist von zwei Wochen widersprechen.

4.2. Wahrung der Vertraulichkeit

(a) Sämtliche Auftragsdaten sind vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich:

(i) die Auftragsdaten angemessen gegen eine Kenntnisnahme durch Unbefugte zu schützen;

(ii) sicherzustellen, dass alle Personen mit Zugang zu den vertraulichen Informationen einer angemessenen gesetzlichen oder vertraglichen Vertraulichkeitsverpflichtung unterstehen; und

(iii) nur Personen Zugriff auf vertrauliche Informationen haben, die für die Erfüllung ihrer Pflichten darauf angewiesen sind, wobei Zugang und Zugriff auf das sachlich und personell geschäftsnotwendige Mass zu beschränken sind (Einhaltung des «need-to-know» Prinzips).

(b) Der Auftragnehmer ist verpflichtet, den Auftraggeber über Anfragen oder Anordnungen von Behörden (z.B. Gerichts-, Straf- und Verwaltungsbehörden) unverzüglich zu informieren, soweit dies nach dem anwendbaren Recht zulässig ist. Er verweist die anfragende Behörde jeweils an den Auftraggeber. Unter Vorbehalt abweichender Weisungen des Auftraggebers ergreift er auf Kosten des Auftraggebers die nach dem anwendbaren Recht möglichen und nicht offensichtlich aussichtslosen Rechtsbehelfe, um eine Offenlegung von Auftragsdaten zu verhindern oder einzuschränken. Ist er verbindlich zur Offenlegung verpflichtet, legt er nur das Minimum an Auftragsdaten offen.

4.3. Meldung von Verletzungen der Datensicherheit

(a) Der Auftragnehmer benachrichtigt den Auftraggeber im Fall einer Datensicherheitsverletzung unverzüglich und spätestens innerhalb von 48 Stunden, nachdem der Auftragnehmer von der Datensicherheitsverletzung Kenntnis erlangt.

(b) Die Mitteilung an den Auftraggeber enthält mindestens die folgenden Angaben (wobei diese gestaffelt zu übermitteln sind, soweit sie zum Zeitpunkt der Benachrichtigung noch nicht vollständig bekannt sind):

(i) Art der Datensicherheitsverletzung;

(ii) betroffene Personen (Kategorie und ungefähre Zahl der betroffenen Personen);

(iii) Art und Umfang der von der Datensicherheitsverletzung betroffenen Personendaten des Auftraggebers (Kategorien und ungefähre Zahl der betroffenen Daten);

(iv) Kontaktperson von Auftraggeber, bei der zusätzliche Auskünfte eingeholt werden können;

(v) erwartete Folgen der Datensicherheitsverletzung für die betroffenen Personen;

(vi) getroffene oder geplante Massnahmen zur Untersuchung und Bewältigung der Datensicherheitsverletzung.

5. Unterauftragnehmer

(a) Zulässigkeit: Der Auftragnehmer ist befugt, Unterauftragnehmer beizuziehen, sofern diese im Einklang mit dem Vertrag und diesem AV-Vertrag beigezogen werden und er mit diesem eine Vereinbarung in Textform getroffen hat, die dem Unterauftragnehmer im Wesentlichen dieselben Pflichten auferlegt, welchen der Auftragnehmer nach diesem AV-Vertrag unterliegt. Beim Beizug von Unterauftragnehmern aus Drittstaaten gilt Ziff. 2(c). Der Auftragnehmer haftet dem Auftraggeber für die Einhaltung der Pflichten der Unterauftragnehmer wie für sein eigenes Verhalten.

(b) Genehmigung:

(i) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsbearbeiter beizuziehen, ist dies dem Auftraggeber möglichst frühzeitig durch ausdrückliche Mitteilung in Textform mitzuteilen. Widerspricht der Auftraggeber der Beauftragung des Unterauftragsbearbeiters durch Mitteilung in Textform innerhalb von 20 Tagen seit Zugang der entsprechenden Mitteilung und ist der Auftragnehmer nicht bereit, auf den Beizug des entsprechenden Unterauftragsbearbeiters zu verzichten, hat jede Partei das Recht, den Vertrag und diesen AV-Vertrag ausserordentlich zu kündigen.

(ii) Als hiermit genehmigte Unterauftragsbearbeiter gelten (i) die im Vertrag ggf. vorgesehenen Subdienstleister, (ii) die dem Auftraggeber vor Vertragsschluss in Textform mitgeteilten Unterauftragnehmer und (ii) die Unternehmen der BKW-Gruppe.

6. Datenschutzrechtliche Kontrollrechte

(a) Der Auftraggeber ist bei Dringlichkeit oder dem Verdacht auf eine Verletzung berechtigt, die dem Auftragnehmer übertragene Verarbeitung von Auftragsdaten in Bezug auf die Einhaltung der anwendbaren Datenschutzvorschriften zu prüfen und einzusehen. Dazu gehört auch die Prüfung der Sicherheit der für Dienstleistungen bereitgestellten IT-Infrastruktur.

(b) Im Rahmen solcher Audits ist der Grundsatz der Verhältnismässigkeit einzuhalten und sind die schutzwürdigen Interessen des Auftragnehmers (namentlich an Geheimhaltung) angemessen zu berücksichtigen. Vorbehältlich einer abweichenden Regelung trägt der Kunde sämtliche Kosten solcher Audits (inklusive nachgewiesene interne Kosten des Auftragnehmers, die bei der Mitwirkung am Audit entstehen).

(c) Im Vertrag allfällig definierte Audit-Rechte sowie gesetzlich zwingend vorgeschriebene Prüfrechte des

Auftraggebers oder seiner Aufsichtsbehörden bleiben vorbehalten.

7. Weitere Unterstützungspflichten

(a) Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Einhaltung seiner Pflichten zur Gewährleistung einer angemessenen Datensicherheit, zur Meldung von Datenschutzverletzungen und zur Durchführung von Datenschutz-Folgenabschätzungen.

(b) Soweit sich eine betroffene Person im Zusammenhang mit datenschutzrechtlichen Ansprüchen (z.B. mit einem Auskunfts- oder Löschbegehren) an den Auftragnehmer wendet, leitet der Auftragnehmer das entsprechende Begehren unverzüglich dem Auftraggeber weiter. Er beantwortet keine solchen Begehren. Er unterstützt den Auftraggeber angemessen bei der Bearbeitung solcher Begehren, ebenso wie bei Mitwirkungspflichten gegenüber von Behörden.

8. Übermittlung ins Ausland

(a) Soweit die Zulässigkeit der Übermittlung von Personendaten durch den Auftragnehmer an den Auftraggeber durch den Einbezug genehmigter Standardvertragsklauseln begründet wird, vereinbaren die Parteien für diese Übermittlung hiermit als Bestandteil des AV-Vertrags die Europäischen Standardvertragsklauseln (SCC; https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0914), allgemeine Bestimmungen und Modul 4. Im Widerspruchsfall gehen die SCC dem Vertrag und diesem AV-Vertrag vor.

(b) (i) Klausel 7 SCC gilt; (ii) Klausel 11 SCC gilt ohne die Option; (iii) bei Klausel 17 SCC gilt das im Vertrag vereinbarte Recht als anwendbar oder schweizerisches Recht, falls das anwendbare Recht nicht regelt; (iv) bei Klausel 18 SCC gilt der Gerichtsstand des Vertrags; (v) Anhang I der SCC richtet sich nach dem Vertrag und Anhang II nach Anhang 1 dieses AV-Vertrags. (v) Untersteht die unter die SCC fallende Übermittlung schweizerischem Datenschutzrecht, sind Verweisungen in den SCC auf die DSGVO auch als solche auf das schweizerische DSG und Verweisungen auf EU-Mitgliedstaaten auch auf die Schweiz zu lesen und ist der EDÖB eine zuständige Aufsichtsbehörde.

9. Ansprechpersonen

(a) Der Auftraggeber gibt dem Auftragnehmer eine oder mehrere Ansprechpersonen für Fragen im Zusammenhang mit diesem AV-Vertrag an.

(b) Der Auftragnehmer gilt als befugt, bis auf Widerruf mit dieser Person zu allen Belangen der Auftragsverarbeitung einschliesslich für Meldungen von Datensicherheitsvorfällen zu kommunizieren.

10. Schlussbestimmungen

(a) Änderungen: Änderungen oder Ergänzungen dieser Vereinbarung bedürfen einer ausdrücklichen Vereinbarung in Textform.

(b) Haftung: Die Haftung aus Verletzungen richtet sich nach dem Vertrag und subsidiär nach den von

Gesetzes wegen geltenden Haftungsregelungen.

(c) Mitteilungen: In diesem AV-Vertrag vorgesehene Mitteilungen müssen jeweils ausdrücklich und in Textform (z.B. per E-Mail) erfolgen, sofern nichts anderes vereinbart ist.

(d) Streitschlichtung: Das anwendbare Recht und der Gerichtsstand richten sich nach dem Vertrag.

Anhang 1: Technische und organisatorische Massnahmen

Stand: April 2026

1. Einleitung

(a) Die nachfolgenden technischen und organisatorischen Massnahmen beschreiben die konkret vom Auftragnehmer im Zusammenhang mit der Verarbeitung der Personendaten und der Erfüllung der Verpflichtungen gemäss dem Hauptvertrag und der Auftragsverarbeitungsvereinbarung zu ergreifen sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(b) Findet die Datenverarbeitung durch einen vom Auftragnehmer beigezogene Unterauftragnehmer statt, sorgt der Auftragnehmer mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Unterauftragnehmer vergleichbare Massnahmen einhalten. Die Beurteilung, ob die nachfolgend beschriebenen technischen und organisatorischen Massnahmen zum Schutz der dem Auftragnehmer anvertrauten Daten angemessen sind, obliegt dem Auftraggeber

2. Zutrittskontrolle

(a) Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

(b) Die Zutrittskontrolle kann die folgenden Massnahmen umfassen: Alarmanlagen, automatischer Meldung an einen Sicherheitsdienst, Elektronische Zutrittssysteme über Magnetkarten, Berechtigungen und Schliesssysteme für sensitive Räume, Datenschutzkonforme Videoüberwachung, Berechtigungsprozess, Besucherregelung, Empfangspersonal sorgfältige Auswahl von Reinigungs- und Wachpersonal.

3. Zugangskontrolle

(a) Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

(b) Die Zugangskontrolle kann die folgenden Massnahmen umfassen: IT-Systeme in eigenständigen, gesicherten Netzwerken, Sicherung durch Benutzerkennung und Passwort, sichere Passwörter gemäss Passwort-Richtlinie, Zwei-Faktor-Authentifizierung, Verschlüsselung Mobiler Endgeräte, Anti-Viren-Software, vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung, Zugänge gemäss Need-to-Know nach vorheriger Freigabe, Sperrung von Zugängen nach Austritt, Regelmässige Prüfung aller Zugangsberechtigungen.

4. Zugriffskontrolle

(a) Massnahmen, die 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.

(b) Die Zugriffskontrolle kann die folgenden Massnahmen umfassen: Nur freigegebene Geräte (PCs, Laptops etc.) können das Netzwerk nutzen, Zugriffe auf Rechner und Anwendungen nur mittels Benutzerkennung und Passwort. Sichere Passwörter gemäss Passwort-Richtlinie, Protokollierung von Zugriffen, Berechtigungskonzept, Zugriffsvergabe nach dem Need-to-Know Prinzip und vorheriger Freigabe, periodische Überprüfung von Berechtigungen, insb. von administrativen Benutzerkonten, begrenzte Anzahl an Administratoren, die die volle Zugriffsberechtigung haben, Vier-Augen-Prinzip bei Spezialanwendungen, alle Mitarbeitenden nehmen an jährlichen Datenschutzschulungen teil, Entsorgung von vertraulichen Daten über zertifizierte Fachentsorger.

5. Trennungskontrolle

(a) Massnahmen, die eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, garantieren.

(b) Die Trennungskontrolle kann die folgenden Massnahmen umfassen: Zutrittsgesicherte Sicherheitsbereiche, Datenverarbeitende Applikationen auf virtualisierten Applikationsservern, Zugriffe gemäss Need-to-Know Prinzip, Trennung der Systeme in Entwicklung, Test, Integration und Produktion, Einsatz von Firewalls, Mandantentrennung, auf die jeweiligen Datensätze angepasste Datenbankrechte und Berechtigungskonzepte, Berechtigungskonzept, Trennung der für verschiedene Zwecke gespeicherten Daten.

6. Eingabekontrolle

(a) Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

(b) Die Eingabekontrolle kann die folgenden Massnahmen umfassen: Speicherung vertrauliche Dokumente, Nachvollziehbarkeit von Zugriffen, Zugriff auf Protokolle durch IT-Administration, Protokolle sind in die Datensicherungsverfahren integriert, Aufbewahrungsfristen, Einrichtung und Verwendung von individuellen Benutzernamen, Vergabe von Zugriffsberechtigungen.

7. Weitergabekontrolle

(a) Massnahmen, die 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.

(b) Die Weitergabekontrolle kann die folgenden Massnahmen umfassen: Zugriff in dedizierte Netzwerkzonen, ausschliesslich über firmeneigene Geräte und VPN-Zugang mit 2-Faktor-Authentifizierung, Daten auf mobilen Geräten sind verschlüsselt, Datenaustausch via SFTP, E-Mail-Verschlüsselung, Entsorgung vertraulicher Unterlagen und elektronischer Datenträger über einen zertifizierten Entsorger.

8. Auftragskontrolle

(a) Massnahmen, die gewährleisten, dass die Verarbeitung von personenbezogenen Daten durch Unterauftragnehmer nur entsprechend den Weisungen des Auftraggebers erfolgt.

(b) Die Auftragskontrolle kann die folgenden Massnahmen umfassen: Vertraulichkeitsverpflichtung, Meldung von Sicherheitsvorfällen, Datenschutz-Folgenabschätzungen, sorgfältige Auswahl von Unterauftragnehmern, Abschluss von Auftragsverarbeitungsvereinbarungen.

9. Verfügbarkeitskontrolle

(a) Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

(b) Die Verfügbarkeitskontrolle kann die folgenden Massnahmen umfassen: Überwachung und Absicherung der Serversysteme, Datensicherungsverfahren und Archivierung, Redundante Systeme, Diebstahlsicherungen, Virenschutz, Firewall/ IDS, Alarmanlagen, Brandschutzvorkehrungen im Serverraum und den Büroräumen, Tests für Datenwiederherstellungen, Feuerlöscher, Notfall-Management, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern.

10. Wiederherstellbarkeit

(a) Massnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.

(b) Die Widerherstellbarkeit kann die folgenden Massnahmen umfassen: Virtualisierte Systeme, Datensicherungen, Redundante Server mit Reservekapazität, Notfallpläne, Übungspläne, Notfallkonzept/ Notfallplan, Audits, Übungen, Notfalldokumentationen.

11. Überprüfung, Bewertung und Evaluierung (Organisationskontrolle)

(a) Massnahmen zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(b) Die Organisationskontrolle kann die folgenden Massnahmen umfassen: Datenschutz-Management bzw. Datenschutz-Organisation, Incident-Response-Management, Datenschutzfreundliche Voreinstellungen, dokumentiertes Verarbeitungsverzeichnis, Schulung von Mitarbeitenden, zentrales Weisungsmanagement.