



Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

Rehm Software GmbH, Großtobeler Straße 41, 88276 Berg
im folgenden Rehm oder Auftragnehmer

und

dem Auftraggeber _____

Rehm Software GmbH
Großtobeler Straße 41
88276 Berg

Telefon +49 751 56020-0
Telefax +49 751 56020-99

E-Mail info@rehm.de
Internet www.rehm.de

Diese Vereinbarung konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus der in der jeweiligen Beauftragung (Erst- sowie sämtliche etwaige Folgebeauftragungen) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Auftragsverhältnis bzw. den Auftragsverhältnissen in Zusammenhang stehen und bei denen Beschäftigte der Rehm oder durch Rehm Beauftragte personenbezogene Daten (im folgenden Daten) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Die Dauer der Auftragsverarbeitung ergibt sich aus dem Auftrag. Der Gegenstand der Auftragsverarbeitung sowie Art und Zweck der Verarbeitung personenbezogener Daten sind im Folgenden angeführt:

Installation, Konfiguration und Wartung von Softwareprodukten sowie Support

Im Rahmen der o. a. Tätigkeit kann ein Zugriff auf IT-Systeme des Auftraggebers erforderlich sein. Hierbei kann ein Zugriff auf personenbezogenen Daten (siehe Daten- bzw. Betroffenenkategorien) nicht ausgeschlossen werden.

Sofern durch den Auftraggeber gewünscht kann die Erbringung von Serviceleistungen auch eine Übermittlung von Datenbankdateien, welche vereinzelt neben technischen Inhalten auch personenbezogene Daten, wie bspw. Namen von an Bauvorhaben oder Planungsmaßnahmen beteiligten Firmen beinhalten, auf die ein Zugriff durch den Supportmitarbeiter nicht ausgeschlossen werden kann. Die Datenbankdateien werden auf den Systemen des Auftragnehmers gespeichert und können auch nach Beantwortung von Supportanfragen für etwaig folgende Anfragen und damit verbundene Analyse Zwecke vorgehalten werden. Der Auftraggeber kann der Speicherung von Datenbankdateien zur Erbringung der Serviceleistung widersprechen. In diesem Fall kann eine Analyse und Fehlersuche nur vor Ort beim Auftraggeber durchgeführt werden.

Mit Beendigung des zwischen den Parteien bestehenden Auftragsverhältnisses insgesamt, nicht jedoch der einzelnen Support-Beauftragung, werden vorgehaltene Datenbankdateien des Auftraggebers gelöscht. Das Auftragsverhältnis endet mit der ordnungsgemäßen Kündigung des Hauptvertrags oder im Falle von Einzelbeauftragungen mit dem Widerspruch zur Speicherung. Der Widerspruch sowie die Kündigung bedürfen der schriftlichen Form oder des elektronischen Formats (Textform).



Eine darüber hinaus gehende Vorhaltung der Dateien findet lediglich im Sinne einer eingeschränkten Verarbeitung für einen definierten Zeitraum in Backup-Systemen statt, wobei sichergestellt ist, dass im Rahmen von Löschersuchen durch Betroffene vernichtete Dateien von einer Wiederherstellung ausgeschlossen sind.

Die Kategorien der personenbezogenen Daten wie auch die Kategorien der Betroffenen sind auf Seite 1 dieser Vereinbarung benannt.

Der Zugriff auf das IT-System des Auftraggebers kann erfolgen:

- vor Ort im Rahmen des Serviceeinsatzes eines Mitarbeiters
- per Fernwartung auf Anfrage des Auftraggebers nach aktiver Freigabe durch dessen Mitarbeiter

Datenarten, die verarbeitet werden:

- Personenstammdaten (z.B. Anrede, Name, Vorname, Adresse, Titel, Funktion)
- Kommunikationsdaten (Telefon, E-Mail)
- Technische Protokolldaten (z.B. Login, IP, Zeitstempel)

Kreis der von der Datenverarbeitung betroffenen Personen:

- Kunden des Auftraggebers
- Beschäftigte des Auftraggebers
- Beschäftigte von Auftraggebern des Auftraggebers
- Beschäftigte von Auftragnehmern des Auftraggebers
- Ansprechpartner von Lieferanten des Auftraggebers
- Andere [Bitte ausführen]

§ 2 Anwendungsbereich und Verantwortlichkeit

- (1) Rehm verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Auftrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an Rehm sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).
- (2) Die Weisungen werden anfänglich durch die Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an die von Rehm bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
- (3) Zur Weisung befugter Personenkreis beim Auftraggeber:

(Funktion oder Organisationseinheit, Telefon, E-Mail)

Weisungsempfänger bei Rehm sind: Service-Mitarbeiter, Vertriebsmitarbeiter und Mitarbeiter der Service-Annahme (Telefon, E-Mail).

Für die Weisung zu nutzende Kommunikationskanäle:

Technische Hotline: +49 751 56020-0

Technischer Mailkontakt: support@rehm.de

§ 3 Pflichten des Auftragnehmers

- (1) Rehm darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Rehm darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- (2) Rehm wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DSGVO) genügen. Rehm hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Das im Anhang beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse bei Rehm dar.

Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die dokumentierte Selbstauditierung der Rehm verwiesen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt Rehm vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

- (3) Rehm unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche von betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Anfallende Kosten können dem Auftraggeber in Rechnung gestellt werden.
- (4) Rehm gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für Rehm tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet Rehm, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

- (5) Rehm unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Rehm trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

- (6) Unser Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen kann unter datenschutz@rehm.de erreicht werden.

- (7) Rehm gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

- (8) Rehm berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt Rehm die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

- (9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

- (10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 10 entsprechend. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen).

- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an Rehm, wird Rehm die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Rehm leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Rehm unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Anfallende Kosten können dem Auftraggeber in Rechnung gestellt werden. Rehm haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

- (1) Rehm weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln (Dokumentierte Durchführung eines Selbstaudits) nach.
- (2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Rehm darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu Rehm stehen, hat Rehm gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf Rehm eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für Rehm grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

- (3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn Rehm weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Als zustimmungspflichtiges Subunternehmerverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und

Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert Rehm den Auftraggeber.

Der Auftraggeber kann der Änderung – innerhalb einer Frist von 14 Tagen nach Bekanntgabe (per E-Mail) – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

Erteilt Rehm Aufträge an Subunternehmer, so obliegt es Rehm, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

Zurzeit sind für Rehm die folgenden Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Derzeit beauftragte zustimmungspflichtige Subunternehmer:

Name	Anschrift	Auftragsinhalt
TeamViewer GmbH	Jahnstr. 30, 73037 Göppingen	Hersteller der Fernwartungssoftware für Supportleistungen
United Hoster GmbH	Max-Eyth-Str. 21, 72622 Nürtingen	Hosting Mailserver und Dateitransfer-Manager für Supportanfragen
ALL-INKL.COM - Neue Medien Münnich	Hauptstraße 68, 02742 Friedersdorf	Support-Anfragen, Anmeldungen zu Veranstaltungen, Kontakt-Anfragen

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

- (1) Sollten die Daten des Auftraggebers bei Rehm durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat Rehm den Auftraggeber unverzüglich darüber zu informieren. Rehm wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen von Rehm – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.



(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Rehm haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer

Anhang – Technische und organisatorische Maßnahmen

1. Vertraulichkeit

Zutrittskontrolle

Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen sind. Das Bürogebäude ist durch eine Alarmanlage gesichert, die über Bewegungsmelder im Gebäude verfügt und mit redundanten Kommunikationsverbindungen mit einem Sicherheitsdienst verbunden ist.

Zum Betreten des Gebäudes wird ein Schlüssel sowie ein Sicherheits-Token benötigt, alle Scharf- und Unscharfschaltungen der Alarmanlage werden protokolliert. Die Vergabe und die Rückgabe von Schlüsseln und Token wird dokumentiert.

Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.

Reinigungskräfte verfügen über Schlüssel und Sicherheitstoken, die keinen Zutritt zum Serverraum gestatten.

Zugangskontrolle

Zugang zu IT-Systemen erfolgt lediglich über entsprechende Zugangsberechtigungen, welche vom Administrator vergeben werden.

Die Passwörter für die dedizierten Benutzeraccounts und sonstiger Konten zur Verwaltung der IT-Infrastruktur (z.B. Domänen-Administrator) sowie zur Verschlüsselung der Datensicherung sind zufallsgeneriert und werden in einem per Master-Passwort verschlüsselten digitalen Passwortsafe gespeichert. Kopien der Passwörter liegen versiegelt in ausgedruckter Form in einem feuerfesten Tresor im Gebäude und werden zudem, ebenso versiegelt, in einem weiteren Tresor in einem separaten Brandabschnitt aufbewahrt.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. im Support tätig sind.

Trennung

Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, wird er diese getrennt von Daten anderer Kunden verarbeiten.

Pseudonymisierung & Verschlüsselung

Fernzugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen mit der Software „TeamViewer“. Der Benutzer auf Seiten des Auftraggebers muss die Verbindung proaktiv einleiten und dem Supportmitarbeiter ein zufallsgeneriertes Passwort mitteilen, ohne das er sich nicht verbinden kann. Der Benutzer auf Seiten des Auftraggebers sieht im Verlauf der Verbindung sämtliche Eingaben und Handlungen des Supportmitarbeiters an seinem eigenen Bildschirm in

Echtzeit. Möglichkeiten zur Aufschaltung auf Systeme des Auftraggebers ohne aktives Zutun der Beschäftigten des Auftraggebers sind organisatorisch ausgeschlossen.

2. Integrität

Eingabekontrolle

Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist.

Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung für den Auftraggeber untersagt.

3. Verfügbarkeit und Belastbarkeit

Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell gesichert werden. Automatische, regelmäßige Integritätstestläufe stellen sicher, dass die Datensicherungen stets intakt und verfügbar sind.

Die tägliche Sicherung erfolgt nach Stand der Technik verschlüsselt auf zwei im Haus befindliche NAS-Systeme. Die Datenträger auf den NAS-Systemen sind jeweils in einem „RAID 6“-Verbund konfiguriert, um vor Datenverlust durch Hardware-Defekten gesichert zu sein.

Vollständige Kopien dieser gesamten verschlüsselten Datensicherung liegen auf weiteren Festplatten, von denen eine Kopie räumlich getrennt in einem feuerfesten Tresor in einem getrennten Raum aufbewahrt wird, der Zugang ist lediglich zwei Personen möglich. Eine weitere Kopie befindet sich in einem feuerfesten Tresor in einem separaten Brandabschnitt. Diese Kopien werden jeweils monatlich zu Monatsbeginn bzw. Mitte des Monats aktualisiert. Eine Langzeitsicherung der Daten erfolgt ebenfalls verschlüsselt auf ein weiteres „RAID 6“-System.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht.

Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Auftragskontrolle



Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Etwaige nach Art. 25 DSGVO erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen.