SEPA - Lastschriftmandat

wiederkehrende Lastschrift

Gläubiger - Identifikationsnummer : DE24ZZZ00000003514

Mandatsreferenz :
(entspricht raw-Kundennummer)

Ich/Wir ermächtigen die GRÜN raw GmbH, Zahlungen von meinem Konto

IBAN: DE _ _ | _ _ _ _ | _ _ _ _ | _ _ _ _ | _ _ _ _ | _ _

BIC _ _ _ _ | _ _ | _ _ | _ _ _

Kreditinstitut _____

mittels Lastschrift einzuziehen. Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die von der GRÜN raw GmbH auf mein Konto gezogene Lastschriften einzulösen. Hinweis: Ich kann/ Wir können innerhalb von acht Wochen, beginnend mit dem Datum der Belastung, die Erstattung des belasteten Betrages verlangen. Es gelten die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen.

(möqlichst bitte einen Firmenstempel verwenden)

Kontoinhaber Strasse und Hausnummer PLZ und Ort	

.....

(Ort, Datum, **Unterschrift)**

Leistungsbeschreibung Cloudarchiv
Anlage zum Basisvertrag

Das Cloudarchiv der GRÜN raw GmbH ist ein eigenständiges elektronisches Archiv für Rechnungen außerhalb der ZR und alle sonstigen Belege oder Dokumente. Es ist unabhängig von der aktuell verwendeten ERP-Software oder der Software des aktuellen Steuerberaters. Gleichzeitig können aus dem Cloudarchiv heraus Daten für Drittsyteme zur digitalen Weiterverarbeitung bereit gestellt werden. Es ermöglicht die Einhaltung der aktuellen deutschen Gesetze hinsichtlich Beweis- und Revisionssicherheit, Dokumentations-Echtheit und Aufbewahrungsfristen (IT-Compliance und GoBD). Es bietet dem Mandanten höchste Sicherheitsstandards wie z. B. eine umfangreiche Protokollierung, sichere Verschlüsselungs-algorithmen und ein kennwortgeschütztes Systemumfeld. Ausschließlich autorisierte Personen können Dokumente einsehen oder bearbeiten. Im Ergebnis werden eine höhere Transparenz sowie eine Steigerung der Produktivität und der Prozessqualität erreicht.

Allgemein

- Das Cloudarchiv basiert auf einem eigenständig zwischen Mandant und GRÜN raw geschlossenen Archivierungsvertrag. Dies dient der Rechtssicherheit bzgl. der Belegablage gegenüber Dritten. Sofern der Zugriff auf das Cloudarchiv über ein Rechnungsportal einer Zentralabrechnung erfolgt, so ist sichergestellt, dass Dritte keinen Zugriff auf diesen Bereich haben.
- Je Anwender und Belegart erfolgt das Zugriffsrecht für den Zugriff (lesen) und die Archivierung (schreiben)
- Die gewünschten Dokumententypen können frei konfiguriert werden. Individuelle Archivordner (Belegarten/Dokumententypen) und Belegfelder je Belegart dienen der Differenzierung. Die Belegfelder werden über Feldtypen (Numerisch, Character, Dezimal, Wertelisten, Datum) definiert.
- Bei der gleichzeitigen Nutzung eines von raw betriebenen Rechnungsportals einer Zentral-abrechnung verknüpfen sich Belegarten wir z.B. Lieferscheine automatisch mit den über die Zentralabrechnung archivierten Rechnungen.
- E-Rechnungen (Zugferd 2. X-Rechnung Stand 08.2024, gültig ab 01.2025) werden auf einem E-Mail-Konto des Mandanten entgegengenommen, an das Rechenzentrum übergeben, dort gemäß EN 16931 validiert, indiziert, optional visualisiert und nach ggfs. ergänzender Kontierung durch den Anwender archiviert.
- Die Archivierung reiner PDF erfolgt dem Upload über manuelle "Verschlagwortung" (Indizierung). Hierdurch wird ein gezielter, eindeutiger und schneller Belegzugriff gewährleistet. Eine OCR-Erkennung ist nicht implementiert und ist bei E-Rechnungen überflüssig.
- für die Archivierung von Belegen aus Vor- bzw. Fremdsystemen kann eine Importschnittstelle genutzt werden. In der Praxis kommt es beispielhaft zur Archivierung von Eingangslieferscheinen, Kostenrechnungen, SEPA-Mandaten, Kundenkontenanträgen, Personalakten, Verträgen etc. .
- Archivierungsdaten lassen sich als Datendatei (z.B. csv-Datei, DATEV-Online) ausgeben. Beispielhaft wäre die Ausgabe einer Datendatei von Kostenrechnungen zum Import in das Buchhaltungsystem.

- Ein integrierter "Workflow" regelt den Bearbeitungsprozess bzw. den Belegfluß in Ihrem Unternehmen, unabhängig von Standort oder Einsatzort des Anwenders.

Technische Voraussetzungen

- Es sind keine Investitionen in Lizenzen oder Hardware notwendig. Das Cloudarchiv wird im GRÜN raw eigenen Rechenzentrum betrieben. Die lokale Verfahrensdokumentation reduziert sich auf die Darstellung der Zugriffsrechte und Tätigkeiten der Anwender
- Benötigt wird ein PC-Arbeitsplatz mit Internetzugang.
- Der Zugang des Mandanten erfolgt über das Internet mittels geschützter Verbindung

Vorbereitende Maßnahmen

- Festlegung der zu archivierenden Dokumententypen (Ordner, z.B. Kostenrechnung)
- Festlegung der Felder (max. 15) die je Beleg zu erfassen sind. (Beispiel: Ordner= Ausgangsrechnungen; Felder=Kunden-Nr., Kundenname, Rechnungs-Nr., Rechnungsdatum, Betrag)
- Abstimmung der Kreditoren-Nr, zur Vermeidung von Redundanzen
- Festlegung der Anwender und deren Zugriffsrechte auf die Ordner.

Schulung

- Schulung Basispaket Archivierung pauschal (½ MT) Systemkonfiguration, Einführung in die ordnungsgemäße Archivierung, Grundlagen zur Anlage von Verzeichnissen und Indexfeldern, Archivierungsvorgang an sich von Belegen wie z.B. Kostenrechnung, Warenrechnung, Ausgangsrechnung.
- Schulung Basispaket Workflow pauschal (½ MT) Umsetzung eines vorhandenen Workflows im Cloudarchiv und Zuordnung der Anwender, nutzerbezogene Rechtevergabe, Datenausgang zur Nutzung der Beleginformation durch Drittsysteme.

Die Schulung der Basispakete erfolgt als Blockschulung online (bspw. via TeamViewer) oder am Standort GRÜN raw. Das Basispaket Workflow setzt das Basispaket Archivierung voraus. Die Nutzung der Hotline setzt eine jeweilige Schulung voraus. Hierüber hinaus gehende Organisationsanalyse, Schulung, Sonderprogrammierung wird gemäß aktueller Preisliste berechnet

Datenauslagerung

Auf Bestellung werden dem Mandanten die archivierten Daten in einem selbsttragenden Archiv auf einem Datenträger mit einer Software zur Visualisierung der Dokumente und Daten (Team-Serv Archiv DiscClient) ausgeliefert und die entsprechenden Daten im Cloudarchiv gelöscht.

GRÜN raw, 21.08.2024

Preisliste Cloudarchiv
Anlage zum Basisvertrag

THEMA	LEISTUNG	PE	€ / PE
Cloudarchiv	Aktivierung, Freischaltung	Einmalig	145,00
	Betrieb und Bereitstellung Archivsystem inklusive Workflow zur GoBD-konformen Archivierung von Rechnungen und frei einrichtbaren Belegarten, inkl. 1 GB Speicherplatz, beliebige Anzahl Anwender	Mandant/Monat	30,00
	Speicherplatz-Erweiterung	je GB/Monat (additiv)	
		bis zum 5. GB	30,00
		ab dem 6. GB	20,00
		ab dem 11.GB	10,00
	Beispiel: 6 GB Speicherplatz (5 x 30,00 + 1 x 20,00 = 170,00€)	ab dem 21.GB	5,00
E-Rechnung	Validierung (EN16931), optional Visualisierung, Indexierung	Rechnung/Stück	0,09
Beratung, Schulung, Progammierung	Die Leistung wird nach tatsächlichem Aufwand berechnet.	MT Stunde	1.380,00 172,50
Hotline	Hotline und Systemunter-stützung in der Geschäftszeit Mo.- Fr. 8:00 bis 17:00 Uhr	Je angefangene ¼ h	42,50
Datenauslagerung	selbsttragendes Archiv (Archiv DiscClient) zur Auslieferung an den Mandanten	je Kalenderjahr und geliefertem Datenträger	38,50

Alle Preisangaben verstehen sich zuzüglich ges. Mwst., Porti, Frachten und Telekommunikationskosten.
Die Rechnungen sind fällig sofort nach Erhalt.
Hiermit verlieren alle bisher veröffentlichten Preislisten die Gültigkeit.
Die Preisliste gilt in Verbindung mit einem Basisvertrag.

Gültig ab 01.09.2024

GRÜN raw GmbH, Am Burgholz 33-35, 52372 Kreuzau-Stockheim
www.raw.de

Auftragsdatenverarbeitung
Anlage zum Basisvertrag

Einleitung, Geltungsbereich, Definitionen
1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber (Mandant) und -nehmer raw (im Folgenden auch „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter der raw oder durch raw beauftragte Unternehmen (Subunternehmer) personenbezogene Daten des Mandanten verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

1. Gegenstand und Dauer der Verarbeitung
Gegenstand und Dauer der Verarbeitung beruhen auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Basisvertrag“)

2. Art und Zweck der Datenerhebung, -verarbeitung oder nutzung:
Art und Zweck der Verarbeitung wird in den Anlagen zum Basisvertrag beschrieben.

3. Pflichten der raw
1. raw verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Mandant angewiesen, es sei denn,raw ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für raw bestehen, teilt raw diese dem Mandant vor der Verarbeitung mit, es sei denn, die Mitteilung ist raw gesetzlich verboten. raw verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
2. raw bestätigt, dass ihr die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Die raw beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
3. Die raw verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
5. Die raw sichert zu, dass die bei ihr zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Die raw trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
6. Im Zusammenhang mit der beauftragten Verarbeitung hat raw den Mandant bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen.
7. Wird der Mandant durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich raw den Mandant im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
8. Auskünfte an Dritte oder den Betroffenen darf raw nur nach vorheriger Zustimmung durch den Mandant erteilen. Direkt an raw gerichtete Anfragen wird sie unverzüglich an den Mandant weiterleiten.
9. Soweit gesetzlich verpflichtet, bestellt raw eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Mandant direkt an den Datenschutzbeauftragten wenden. Die raw teilt dem Mandant die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt raw dem Mandant mit.
10. Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR und der CH. Jegliche Verlagerung in einem anderen Drittland darf nur mit Zustimmung des Mandanten und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

4. Technische und organisatorische Maßnahmen
1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.
2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat raw in eigener Entscheidung umzusetzen.
3. Soweit die getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht oder nicht mehr genügen, benachrichtigt raw den Mandant.
4. Kopien oder Duplikate werden ohne Wissen des Mandanten nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen und Datensicherungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
5. Die Verarbeitung von Daten in Privatwohnungen ist ausgeschlossen.
6. Dedizierte Datenträger, die vom Mandant stammen und zur Verfügung gestellt werden, werden besonders gekennzeichnet. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden nur nach gesonderter Kennzeichnung und separater Beauftragung durch den Mandanten von raw dokumentiert.
7. Die raw führt einen regelmäßigen Nachweis der Erfüllung ihrer Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen. Der Nachweis ist dem Mandant auf Anforderung einmal jährlich zu überlassen. Der Nachweis wird in pflichtgemässen Ermessen der raw erbracht.

5. Regelungen zur Berichtigung, Löschung und Sperrung von Daten
1. Im Rahmen des Auftrags verarbeitete Daten wird raw nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Mandanten berichtigen, löschen oder sperren.
2. Den entsprechenden Weisungen des Mandanten wird raw jederzeit und auch 12 Monate über die Beendigung dieses Vertrages hinaus Folge leisten.

6. Unterauftragsverhältnisse
1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Mandanten im Einzelfall zugelassen.
2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt werden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Mandant erhält auf Verlangen Einsicht in die relevanten Verträge zwischen raw und Subunternehmer.

3. Die Rechte des Mandanten müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Mandant berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
4. Die Verantwortlichkeiten der raw und des Subunternehmers sind eindeutig voneinander abzugrenzen.
5. Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
6. Die raw wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
7. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich raw dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Die raw hat dem Mandant die Dokumentation auf Verlangen vorzulegen.
8. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR sowie der CH erbringen, ist nur bei Beachtung der in Kapitel 3 (10) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Die raw teilt dem Mandant mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
9. Die raw hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Mandant auf Verlangen vorzulegen.
10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür raw gegenüber dem Mandant gemäss den Bestimmungen des Dienstleistungsvertrages.
11. Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Mandant genehmigt. Die hier niedergelegten sonstigen Pflichten der raw gegenüber Subunternehmern bleiben unberührt.
12. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Vernichtung von Papierdokumenten, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht der raw, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

7. Rechte und Pflichten des Mandanten

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Mandant verantwortlich.
2. Der Mandant erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Mandant unverzüglich dokumentiert bestätigen.
3. Der Mandant informiert raw unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. Der Mandant ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen bei raw in angemessenem Umfang durch berufsbedingt zur Verschwiegenheit verpflichtete und sachkundige Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort, zu kontrollieren. Den mit der Kontrolle betrauten Personen ist von raw soweit erforderlich und unter Beachtung anderer Vorschriften Zutritt und Einblick zu ermöglichen. Die raw ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
5. Kontrollen bei raw haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Mandant zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten der raw, sowie nicht häufiger als alle 12 Monate statt. Soweit die raw den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 4 (7) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8. Mitteilungspflichten

1. Die raw teilt dem Mandant Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 Datenschutz-Grundverordnung zu enthalten.
2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße der raw oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
3. Die raw informiert den Mandant unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4. Die raw sichert zu, den Mandant bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9. Weisungen

1. Der Mandant behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
2. Mandant und raw benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.
3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
4. Die raw wird den Mandant unverzüglich darauf aufmerksam machen, wenn eine vom Mandant erteilte Weisung ihrer Meinung nach gegen gesetzliche Vorschriften verstößt. Die raw ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Mandant bestätigt oder geändert wird.
5. Die raw hat ihr erteilte Weisungen und deren Umsetzung zu dokumentieren.

10. Beendigung des Auftrags

1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Mandanten hat der raw die im Auftrag verarbeiteten Daten nach Wahl des Mandanten entweder zu vernichten oder an den Mandant zu übergeben und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandenen Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 01.
2. Die raw ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3. Die raw hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Mandant auf Verlangen vorzulegen.
4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch raw den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende

hinaus aufzubewahren. raw kann sie zu ihrer Entlastung dem Mandant bei Vertragsende übergeben.

11. Vergütung der raw

Die Vergütung der raw ist abschließend im Basisvertrag geregelt, wenn dieser nach dem 24.05.2018 abgeschlossen wurde. Wurde der Basisvertrag vor dem 25.05.2018 geschlossen, so ergibt sich eine gesonderte Vergütung und Kostenerstattung im Rahmen dieses Vertrages gemäss den im Basisvertrag geregelten Stundensätzen.

12. Haftung

1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Mandant und raw als Gesamtschuldner.
2. Der Mandant trägt die Beweislast dafür, dass ein Schaden Folge eines von raw zu vertretenden Umstandes ist, soweit die relevanten Daten von raw unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Mandant raw auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen die raw erhoben werden. Unter diesen Voraussetzungen ersetzt der Mandant der raw ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
3. Die raw haftet dem Mandant für Schäden, die raw, ihre Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen. Es gelten die Haftungsbeschränkungen des Basisvertrages.
4. Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Mandant erteilten Weisung entstanden ist.
5. Strafen sind vom Ersatz als Schaden ausgeschlossen.

13. Sonderkündigungsrecht

1. Der Mandant kann den Basisvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß der raw gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn raw die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14. Sonstiges

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2. Sollte Eigentum des Mandanten bei raw durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat raw den Mandant unverzüglich zu verständigen.
3. Für Nebenabreden ist die Schriftform erforderlich.
4. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 – technische und organisatorische Maßnahmen (TOM)

siehe gesondertes Dokument

Anlage 2 – Zugelassene Subdienstleister

keine

Anlage 3 – Weisungsberechtige Personen / Datenschutzbeauftragter

siehe Basisvertrag

Datenschutzbeauftragter :

datenschutzbeauftragter@raw.de

Datenschutz und Datensicherheit

technische und organisatorische Maßnahmen zum Schutz von Daten

Änderungshistorie

Version	Status	Datum	Autor	Bemerkungen
1.3		24.11.14	tf	Vervollständigung
1.4		18.11.15	tf	Vervollständigung
1.5		08.11.16	tf	Vervollständigung
1.6		02.11.17	tf	Vervollständigung
2.0		10.01.18	tf	Berücksichtigung DSGVO
2.1		20.11.19	tf	Vervollständigung
2.1		12.11.20	tf	Keine Veränderung
2.1		15.12.21	tf	Keine Veränderung
2.1		23.11.22	tf	Keine Veränderung
2.2		30.10.23	tf	Vervollständigung
2.3		01.07.24	tf	Vervollständigung

Inhaltsverzeichnis

Einleitung

Im nachfolgenden Bericht werden die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit nach Artikel 32 DSGVO (Verordnung EU 2016/679 vom 27.04.2016) bei der GRÜN raw GmbH (kurz: raw) aufgelistet und erläutert.

Die hier beschriebenen Maßnahmen werden in der jährlich stattfindenden Prüfung zum IKS (PS 951 Typ 2 und ISAE 3402 Type 2), die durch ein unabhängiges Wirtschaftsprüfungsinstitut durchgeführt wird, untersucht und gegebenenfalls notwendige Veränderungen definiert.

Darüber hinaus werden die Maßnahmen durch den externen Datenschutz-beauftragten der raw geprüft.

Maßnahmen zur Zutrittskontrolle

Gebäude

raw ist ein Systemhaus mit Dienstleistungsrechenzentrum. Das freistehende Unternehmensgebäude ist nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gebaut und eingerichtet worden und erfüllt mit diesen Konzepten die Basis für eine geschützte Datenverarbeitung. Zu den eingerichteten Maßnahmen gehören :

- Großtresore (in Massivbauweise) und Brandschutztresore
- Alarmsysteme, die auf einen Sicherheitsdienst aufgeschaltet sind
- Zutritt zu den Etagen mit Datenschutzrelevanz erfolgt per Schlüssel und Code-Karte und wird durch Überwachungskameras protokolliert
- Einbruch- und Brandmeldeanlagen
- Brandlöschanlage
- Das Gebäude der raw wird 24 Stunden täglich sicherheitsüberwacht und ist mit technischen Maßnahmen zur Abschreckung und Alarmierung ausgestattet. Die Alarmierung unterliegt einem differenzierten Alarmplan.

Mitarbeiter

Die Mitarbeiter sind schriftlich über die Handhabung des Zutritts zu den Räumen mit Datenschutzrelevanz informiert und verpflichtet worden. Darüber hinaus findet eine regelmäßige Prüfung der Einhaltung durch die Geschäftsleitung statt. Den Mitarbeitern sind die Folgen der Nicht-Einhaltung der Richtlinien bekannt.

Die Richtlinien für die Mitarbeiter erstrecken sich ebenfalls auf den Umgang mit Schlüssel und Codekarte.

Eine detaillierte Vorgehensbeschreibung für das Hinterlassen und Verschließen von Gebäudeteilen ist den Richtlinien für Mitarbeiter ebenfalls beigefügt.

Externe

Ausnahmen des Zutritts sind nur für bekannte Serviceunternehmen und deren bekannte Mitarbeiter in Begleitung eines Mitarbeiters der raw für den Zuständigkeitsbereich erlaubt. Das Auftreten eines solchen Mitarbeiters eines Serviceunternehmens bei raw erfolgt grundsätzlich nur bei vorheriger Anforderung durch raw. In einem Zutrittsprotokoll für den Rechenzentrumsbetrieb werden externe Zugänge aufgenommen und durch den begleitenden internen Mitarbeiter bestätigt.

Darüber hinausgehende Ausnahmen sind in seltenen Fällen nur durch die Geschäftsführung und nur mit deren Begleitung zugelassen.
Gäste werden über das Sekretariat im öffentlichen Gebäudebereich entgegengenommen.

Tresore

Die Großtresore können nur durch eine Schlüssel/Zahlenkombination von berechtigten Mitarbeitern des Zuständigkeitsbereichs geöffnet werden.

Die Datensicherungstresore sind ganztägig geschlossen und werden nur für den kurzen Moment des Wechsels von Sicherungsmedien geöffnet und hiernach wieder verschlossen. Die Sicherungsmedien befinden sich innerhalb der Großtresore in hierin stehenden Brandschutztresoren.

Rechenzentrum

Alle datenhaltenden Server- und Speichersysteme sind im Rechenzentrum untergebracht. Dieser Raum befindet sich in einem eigenen Schließbereich und wird sicherungs- und schlüsseltechnisch nur für administrative Tätigkeiten der Systemadministrationsabteilung und zum Zwecke des Wechsels der Datensicherungsmedien geöffnet. Dieser Raum ist fensterlos und ist bautechnisch ein Stahlbetonmantel.

Zutrittsberechtigungen

Die Vergabe von Zutrittsberechtigungen wird über den personalverantwortlichen Mitarbeiter der raw mit der Geschäftsleitung definiert und unter folgenden Gesichtspunkten vergeben :

- Zutrittsnotwendigkeit

- Zutrittshäufigkeit
- Einschätzung eines Zutrittsrisikos
- Abwägung von Alternativen

Maßnahmen zur Zugangskontrolle

Zugang (Passwörter)

Der Zugriff auf Arbeitsplätze, Serversysteme oder Anwendungen erfolgt grundsätzlich über Benutzer-Passwort-Kombinationen.

Die Mitarbeiter der einzelnen Abteilungen haben jeweils nur eingeschränkten Rechner- und Datenzugriff, entsprechend ihrer Verantwortlichkeit.

Im Rahmen des Prozesses der Verarbeitung von Adressdaten (z.B. Rechnungsbelegen, Mahnungen) bis zur Archivierung und Bereitstellung für das Rechnungsarchiv bzw. für den Postversand, werden diese überwiegend automatisiert verarbeitet.

Auf Grund der Verteilung von Aufgaben innerhalb des Gesamtprozesses auf verschiedene Abteilungen, ist eine technische Abgrenzung der Zugänge jeweils auf den entsprechenden Arbeitsbereich beschränkt.
Eine Authentifizierung für den Zugriff auf Daten aus dem Prozess erfolgt auch hier grundsätzlich nur über Benutzername-Passwort-Kombinationen.

Nach 5-maligem erfolglosem Anmeldungsversuch wird die Möglichkeit zur erneuten Eingabe der Benutzer-Passwort-Kombination für 24 Stunden gesperrt.

Nach 10-maligem erfolglosem Anmeldungsversuch an den Rechnungsportalen für die Mitglieder von Kooperationszentralen oder Kooperationszentralen wird die Möglichkeit zur erneuten Eingabe der Benutzer-Passwort-Kombination bis zum nächsten Tag gesperrt

Für jeden Mitarbeiter der raw wurde eine eigene Active Directory Benutzeranmeldung vergeben.

Sollte ein Mitarbeiter seinen Arbeitsplatz vorübergehend verlassen, ohne diesen für den Zugang Dritter gesperrt zu haben, so wird nach 20 Minuten automatisch eine Sperre des Systems durchgeführt.

Verschlüsselung

Zur Gewährleistung der Vertraulichkeit der Daten auf dem Archivserver werden interne Verschlüsselungstechniken eingesetzt, die die Daten in eine „unleserliche“, das heißt nicht interpretierbare Zeichenfolge wandeln.

Auch für die notwendigen Datensicherungen findet eine Verschlüsselung nach aktuellem Standard statt.

Durch eine für den Server bereitgestellte digitale Verschlüsselung werden die zwischen den Mitgliedern und dem Archiv-Server geöffneten Internet-Verbindungen als gesicherte Verbindungen (HTTPS: Hypertext Transfer Protocol secure) betrieben (Mitgliederportal).

Aktualisierung

Windows-Plattformen und Linux-Plattformen werden über einen zentralen Patch-Management Server auf dem neuesten Patch-Level gehalten.

Die Aktualisierung von Virensignaturen erfolgt stündlich über den zentralen Viren-Management-Server, hierbei greifen die Arbeitsplatzrechner der Mitarbeiter automatisch auf den Viren-Management-Server zu.

Maßnahmen zur Zugriffskontrolle

Berechtigung

Ein Zugriff auf Daten- und Belegbilder im Verarbeitungsablauf des Rechenzentrumsbetriebes für Kunden der raw oder für dritte Fremde ist nicht eingerichtet.

Jeder am Prozess beteiligte Mitarbeiter der raw hat nur die für seinen Prozessablauf erforderlichen Zugriffsrechte, die durch den hohen Automatisierungsgrad der Datenverarbeitung weiter beschränkt wird.

Sicherung und Aufbewahrung

Die tägliche Datensicherung aller Systeme erfolgt von Brandabschnitt **I** nach Brandabschnitt **II** und zusätzlich in ein anderes Gebäude. Volle Sicherungsmedien werden in hierfür vorgehaltenen Brandschutztresoren untergebracht.

Bei Ausfall einer Firewall übernimmt automatisch eine zweite Firewall im Cluster die Aufgabe des ausgefallenen Gerätes ohne Zeitverzug. Die Konfigurationsdaten der Firewalls werden regelmäßig gesichert

Wenn Anwendungsserver wie Web, AS2, FTP, Print oder Domain Server ausfallen, dann werden alternative Rechnersysteme unter Verwendung der Daten-/Systemsicherung kurzfristig eingerichtet und in Betrieb genommen. raw verfügt im eigenen Mitarbeiterumfeld über die hierfür notwendigen Spezialisten für Betriebssysteme, Datenbanken und Hardware.

Zum Betrieb eines Rechenzentrums gehört selbstverständlich ein Datensicherungskonzept. Es sieht zum einen ein routinemäßig durchgeführtes Backup-Verfahren vor, das den Bestand gesicherter Daten aktuell hält. Zum anderen gehört ein Disaster-Recovery-Verfahren dazu, dass im Notfall die Wiederherstellung der Systeme und des Datenbestandes unterstützt.

Wochentags werden alle Systeme (Daten, Konfigurationen, Programme) inkrementell gesichert, d. h., es werden die Änderungen des Tages berücksichtigt. Die Primärsicherungen (Backups der Produktionsumgebung, Brandabschnitt I) erfolgen grundsätzlich in einen per Glasfaserkabel angebundenen deduplizierten Festplattenspeicher in einem anderen Gebäude. Erst in einem zweiten Schritt werden die Daten dann von dort auf Bänder geschrieben (Brandabschnitt II im Hauptgebäude).

An Wochenenden werden bei ansonsten gleichem Verfahren Vollsicherungen durchgeführt.

Das Operating prüft werktäglich das Magazin des Bandroboters auf volle Bänder. Volle Bänder werden in den Brandschutztresor ausgelagert und freie Bänder ins Magazin eingelegt.

Der Brandschutztresor erfüllt die Brandschutznormen für Datenträger. Er steht überdies in einem separaten, durch eine massive Panzertür gesicherten Raum, der seinerseits hohen Brandschutzforderungen genügt.

Der Bandroboter mit dem Medienmagazin steht in einem zweiten, in gleicher Weise abgeschotteten und gesicherten Raum.

Rückhaltezeit für Daten im deduplizierten Festplattenspeicher

Die Rückhaltezeit für Daten im deduplizierten Festplattenspeicher beträgt grundsätzlich 30 Tage. Innerhalb dieser Zeit sind Wiederherstellungen taggenau, sehr schnell und ohne Medienhandhabung möglich.

Rückhaltezeit für Daten auf Bändern

Der 30-Tage-Dedup-Speicher wird täglich zur höheren Absicherung auf Bänder gesichert.

Darüber erfolgt für längerfristig aufzubewahrende Daten die Erstellung von Monats-, Quartals- und Jahresauslagerungen. Monatsauslagerungen werden 1 Jahr lang zurückgehalten, Quartals- und Jahresauslagerungen 10 Jahre lang.

Netzwerk

Das Netzwerk ist in Sicherheitssegmente unterteilt, der Zugriff auf die Systeme ist durch eine moderne Infrastruktur genau geregelt und elektronisch überwacht. Ein Zugriff auf Daten ohne Zugriffsberechtigung ist nicht möglich.

Maßnahmen zur Weitergabekontrolle

Sicherungsbänder

Die Bänder werden morgens vom zuständigen Operator aus den Laufwerken entnommen und unmittelbar in die Brandschutztresore eingelagert. Eine Zwischenlagerung der Bänder findet nicht statt.

E-Mail

Der Versand von E-Mails mit Belegdaten erfolgt nur an registrierte Adressen. Jeder Versand wird protokolliert und abhängig vom Schutzgrad der Daten in einem ZIP-Archiv verschlüsselt versandt.

Datenverarbeitung

Im Rahmen des Prozesses der Verarbeitung von Eingangsdaten bis zur Bereitstellung beim Kunden der raw oder dem vom Kunden bestimmten Empfängern, stehen die Daten nur am Prozess beteiligten Mitarbeitern der raw zur Verfügung. Nur durch die automatisierte Übertragung von definierten Daten in für die Kunden der raw bereitgestellten kundenbezogenen Verzeichnissen oder durch den Versand von Unterlagen auf dem Postweg (UPS, Dt. Post AG) erhalten berechtigte Empfänger Daten aus dem Verarbeitungsprozess.

Im Verarbeitungsprozess durchlaufen Daten verschiedene Stationen auf verschiedenen Rechnern. Auf diesen Rechnern befinden sich die Daten in Zwischenformaten. Den Zugriff auf diese Rechner und damit auf diese Daten haben nur raw-Mitarbeiter mit administrativen Rechten auf den Servern.

Unabhängig von den Zugriffsmöglichkeiten sind alle Mitarbeiter zur Geheimhaltung verpflichtet. Jeder Mitarbeiter hat eine Verpflichtungserklärung unterschrieben, dass er sich nach den Vorschriften der Datenschutzgrundverordnung verhält und darüber hinaus Daten und Informationen vertraulich behandelt.

Leitungsverschlüsselung

Datenübermittlungen an raw werden als Nachweis für die Verbindlichkeit von Transaktionen protokolliert.

Zur Sicherung der Integrität gegen den Zugriff von außerhalb des Gebäudes schützen Firewall- und Viren-Scanning Systeme.

Zum Schutz von Übertragungsverbindungen zwischen dem Kunden und raw werden VPN (virtual private network) Verbindungen bereitgestellt.

Darüber hinaus stellt raw einen FTP-Server zur Bereitstellung und Übergabe von Daten- und Belegbildern zur Verfügung. Die Sicherheit der Daten beim Transport zwischen den Systemen wird durch den Einsatz von FTPs (File Transfer Protokoll secure) gewährleistet.

Maßnahmen zur Eingabekontrolle

Rechenzentrumsbetrieb

Alle Eingaben zur Job-Steuerung auf dem zentralen Verarbeitungsserver des Operatings werden durch ein Systemprotokoll aufgezeichnet.

Maßnahmen zur Auftragskontrolle

Auftrag und Organisation

Der Kunde beauftragt die raw zur Durchführung des Druckservice.

Die für die Erbringung der Auftragsdienstleistung erforderlichen Daten/Belegbilder werden seitens des Auftraggebers(durch das dort eingerichtete Programmsystem) in hierfür festgelegte „Verzeichnisse“ abgelegt.
Die für den Auftraggeber zugänglichen Verzeichnisse sind auf Grund der Rechtevergabe nur für diesen verwendbar. Darüber hinaus können von ihm keine anderen „Verzeichnisse“ wahrgenommen, eingesehen oder verändert werden.

Eingestellte Daten werden von hierfür eingerichteten Prozessen (Programmen) wahrgenommen und zur Verarbeitung den Folgeprozessen zur Verfügung gestellt. Des weiteren werden die Daten in dieser Verarbeitungskette auf Auftragskonformität überprüft.

Der Kunde erhält als Rückgabe aus diesem Druckprozess Auszüge von Daten(keine Adressdaten) und Belegbilder bereitgestellt.

Die konkreten Regelungen und Weisungen zur Verarbeitung von Daten und Belegen sind im Dienstleistungsvertrag der raw und in den ergänzenden Datenschutzbestimmungen geregelt. Der Auftraggeber vermittelt ausschließlich Adressdaten, die im Zusammenhang mit der von ihm erbrachten Dienstleistung gegenüber seinen Kunden zur Erfüllung seiner gesetzlichen Pflicht zur Führung einer Buchhaltung und zur Erstellung von Belegen erforderlich sind.

Alle an der Verarbeitung von Daten in jeglicher Form beteiligten Personen sind über die Notwendigkeiten des Datenschutzes aufgeklärt und über die Folgen der Zuwiderhandlung informiert.

Dienstleistungsvertrag Mandant

Der Dienstleistungsvertrag Mandant wird zwischen dem Mandanten(Auftraggeber) und dem EDV-Dienstleistungsunternehmen raw(Auftragnehmer) abgeschlossen.

Der Vertrag regelt die Zusammenarbeit des Mandanten mit raw in der Durchführung der von raw zu erbringenden Leistungen.

Organisation der Informationssicherheit

Neben den schon erläuterten Maßnahmen zum Schutz von Daten und zur Sicherstellung der Informationssicherheit, werden weitere Regeln in der jedem Mitarbeiter persönlich ausgehändigten Betriebsvereinbarung in welcher konkrete Vorgaben zur Betriebs- und Datensicherheit hinterlegt sind (u.a. der Umgang mit mobilen Geräten) sowie eine Erweiterung der Betriebsvereinbarung mit Vorgaben für die Handhabung des Umfeldes „Telearbeitsplatz“.

In der laufenden Projektarbeit werden die Maßnahmen zur Sicherstellung der Informationssicherheit darüber hinaus durch die Beteiligung des Datenschutzkoordinators des Unternehmens in der Projektplanung und beim Deployment berücksichtigt.

Der Schutz von Daten, insbesondere von Daten natürlicher Personen steht im Vordergrund jedes Handelns von Mitarbeitern im Unternehmen. Dies wird auch durch laufende Kontrollen der Vorgaben durch die Geschäftsleitung unterstützt und die Wahrnehmung der Mitarbeiter für die Wichtigkeit der Einhaltung der Vorgaben hierdurch gefördert.

Entwicklung und Wartung

Bei der Programmentwicklung werden gemeinsam mit dem Kunden Anforderungen (Change und Feature Requests) erstellt. Die dort getroffenen Vereinbarungen werden dokumentiert und dem Change-Management der raw zugeführt.

Neben der zielgerichteten Änderung von Programmen auf Anforderung eines Kunden werden die Programme auch im Rahmen ihrer Wartbarkeit in unregelmäßigen Abständen verändert, um etwa bekannten, regelmäßigen Störungen automatisiert zu begegnen. Andere Gründe hierfür können in Veränderungen von Hardware- oder Betriebssystemplattformen der verarbeitenden Systeme begründet sein. Auch diese Programmänderungen werden in Change Requests dokumentiert.

Datenschutz

Durch laufende Kontrollen unabhängiger Wirtschaftsprüfer (IKS PS 951 Typ 2 und ISAE 3402 Type 2) und auftragsspezifische Weisungen an die Mitarbeiter durch die Geschäftsleitung, sowie die Abstimmung des Verhaltens im Umgang mit dem Datenschutz unter Einbindung des Datenschutzbeauftragten wird der Umgang mit dem Datenschutz ständig verifiziert.

Maßnahmen zur Verfügbarkeitskontrolle

Vollständiges Backup- und Recovery-Konzept

Disaster-Recovery-Verfahren (DR) / Notfallkonzept

Bei einem kompletten Ausfall von Systemen greifen Organisationsanweisungen für den Notbetrieb. Ein ausgearbeitetes Notfallkonzept regelt detailliert die Maßnahmen im Störfall. Es definiert, was Störfälle sind, welche Personenkreise zu benachrichtigen sind (Entscheider und Supportmitarbeiter von Systemherstellern oder auch Kunden), welche technischen und organisatorischen Maßnahmen zu treffen sind und wie der reguläre Betrieb nach Ende der Störung wieder hergestellt wird.

Die meisten der im Prozess eingesetzten Server sind virtualisiert. Deren Images werden regelmäßig gesichert, sodass im DR-Fall die Wiederherstellung eines kompletten Servers mit Betriebssystem, Konfiguration und Daten durch Rücksicherung des Images in kürzester Zeit realisierbar ist.

Die wenigen Server, die nicht virtualisiert sind, werden mit klassischen Verfügbarkeitsmethoden verwaltet. Redundanz bei den Festplatten (RAID-Systeme) und Backups auf Magnetbänder erlauben die vollständige Wiederherstellung.

Archivierung (Sicherung)

raw schützt archivierte Daten in verschiedener Hinsicht. Das beginnt beim Grundschutz gemäß BSI-Vorgaben durch

- massive Bauweise, verschiedene Brandschutzabschnitte
- Großtresore
- Alarmsysteme,
- Zutrittsschutz,
- Zutrittsüberwachung

Nach außen hin sind die Systeme softwaretechnisch durch Firewalls mit strikt restriktiver Konfiguration geschützt.

Intern erfolgt der Zugriff grundsätzlich über Benutzer-Passwort-Kombinationen. Die Mitarbeiter der einzelnen Abteilungen haben jeweils nur eingeschränkten Datenzugriff, entsprechend ihrer Verantwortlichkeit.

Die wesentlichen Daten werden in Datenbanken verwaltet, die nur durch automatisierte Prozesse verändert werden. Die Funktionalität der Programme wird in definierten Prüfverfahren sichergestellt.

Das Archivierungsverfahren ist zentraler Bestandteil der von raw erbrachten Dienstleistung.

Die Archivierung (Sicherung) ist fast vollständig automatisiert, und der automatische Prozessablauf unterliegt der ständigen elektronischen und optisch visualisierten Überwachung.

Viren, Firewall und Spam-Filter

Das Rechenzentrum ist mit einer zentralisierten Firewall (CheckPoint) im Cluster und einer zentralen und dezentralen Virenprüfung ausgestattet. Die Virensignaturen werden automatisiert aktualisiert und von Mitarbeitern der Systemüberwachung kontrolliert. Alle Zu- und Abgänge im Hause raw werden hierüber gesteuert. Das System ist redundant ausgelegt.

Auf dem System Management Server ist eine Antivirus Management Konsole eingerichtet. Alle Windows-basierten, raw-eigenen Client und Server Systeme werden von hier aus mit G-Data Antivirus Software ausgestattet und stündlich aktualisiert. Die Linux-basierten Server Systeme werden mit Bitdefender Software ausgestattet und aktualisiert.

Alarme werden unmittelbar per E-Mail an die Gruppe der Systemadministratoren verschickt.

Darüber hinaus werden alle Datenträger, die von außen in die Firmenorganisation eingebracht werden, durch einen hierfür bereitstehenden Stand-Alone Virenprüfrechner im Sekretariat überprüft und verantwortlich freigegeben. Die Aktualisierung des Rechners erfolgt täglich. Alle Mitarbeiter sind über die Betriebsvereinbarung an das Prozedere gebunden.

Bei Ausfall einer Firewall übernimmt automatisch ein zweites System im Cluster deren Aufgaben. Die Konfigurationsdaten der Firewalls werden regelmäßig gesichert

Neben der Virenüberwachung wird auch ein Mailserver mit restriktiver Spamfilterung (G-Data MailSecurity) eingesetzt. Die Filterung erfolgt über ein selbst lernendes System, welches mit diversen Rechnern im Internet zur Aktualisierung der Spamregeln Kontakt aufnimmt. Nur freigegebene Mails werden an den Mailempfänger übermittelt.

Festplattenspiegelung

Im Rechenzentrum der raw werden alle Daten auf Plattensystemen im Raid-Verfahren gespeichert. Der Austausch defekter Platten erfolgt i.d.R. im Hot-Plug-Verfahren ohne Unterbrechung des Produktionsbetriebes.
So kann neben einer störungsfreien Arbeit der Anwender an den Systemen auch ein zeitnaher Wechsel der Platten vorgenommen werden.

Iin den eingesetzten Plattensubsystemen werden ebenfalls Hot-Spare-Platten eingesetzt, die das Risiko eines Datenverlustes bei Plattenausfall zusätzlich

reduzieren. Der Zugriff über die Plattensubsysteme erfolgt über einen redundant ausgelegten Switch.

USV (Unterbrechnungsfreie Strom Versorgung)

Bei kurzfristigem Stromausfall bis zu zwei Stunden werden alle Systeme des Rechenzentrums über eine unterbrechungsfreie Stromversorgungsanlage (USV) weiterbetrieben. Würde innerhalb dieser Zeit keine Notstromversorgung eintreten, so werden die Systeme nach Ablauf dieser Frist automatisch und geregelt herunter gefahren, sodass keine Gefährdung der Systeme oder hierauf befindlicher Daten zu befürchten ist.

Notstromaggregat (Stromversorgung bei Ausfall des öffentlichen Netzes)

Innerhalb von 1 Minute nach Eintreten einer Stromunterbrechung im öffentlichen Netz wird das komplette Firmengelände über ein Notstromaggregat dauerhaft bis zur Wiederherstellung der öffentlichen Stromversorgung versorgt. Das System wird automatisch in Betrieb genommen und ebenfalls automatisch, bei Wiederkehr der öffentlichen Stromversorgung, in den Bereitschaftsmodus zurückgesetzt.

Brandlöschanlage

Der gesamte Rechenzentrumsbereich ist mit einer Brandlöschanlage ausgestattet. Bei dieser Anlage wird bei Detektion einer Rauch-/Brandquelle innerhalb von Sekunden eine Flutung der Räume mit Inergen-Löschgas ausgelöst.

Maßnahmen zum Trennungsgebot

Um eine Absicherung und Fehlverarbeitung von Daten- und Belegbildern zu vermeiden, werden bei raw mehrere parallel verwendete Verfahren zur Trennung eingesetzt.

- Mandanten-Nr

  Die Mandanten-Nr. im zu verarbeitenden Datenbestand sorgt für eine eindeutige Zuordnung zum jeweiligen Auftraggeber. Alle Programme der raw nutzen die Mandanten-Nr. um die jeweiligen Besonderheiten zu berücksichtigen und eine Fehlzuordnung in der Verarbeitung zu verhindern. Die Mandanten-Nr. wird neben der Trennung durch Verzeichnis- oder Ablagestrukturen als zusätzliches Kriterium der Datentrennung eingesetzt.

.

- Separate Speicherbereiche (Datenbanken / Pools)

  Die Belegbilder und Belegdaten eines Auftraggebers (Mandanten) werden für kritische Prozesse in eigenständigen Datenbanken und Speicherbereichen gehalten. Über diese Speichersystematik ist eine eindeutige Trennung der gespeicherten Daten gegeben.

- Eigenständige Prozessabläufe

  Zusätzlich zur Datentrennung erfolgt auf Grund spezifischer Vereinbarungen (Dienstleistungen) mit dem Auftraggeber auch eine Trennung einzelner Prozessabläufe.

- Dedizierte mandantenbezogene Ablagestrukturen mit automatisierter Weiterverarbeitung

  In Abhängigkeit vom Auftraggeber werden Daten- und Belegbilder in eigenen Verzeichnis- und Ablagestrukturen gespeichert.

Maßnahmen zur Verwaltung der Werte

Inventarisierung und Verantwortlichkeit

Eine Inventarisierung der Dienste und Hardwarekomponenten erfolgt über das eingesetzte Monitoring Tool Check_MK. Dort werden die aktuellen Dienste und Hardwareteile überwacht und ggfls. bei Überschreitung von definierten Grenzen Meldungen erzeugt, die von den verantwortlichen Mitarbeitern bearbeitet werden.

Die Systeme liegen in der Verantwortlichkeit der Mitarbeiter der Abteilung Betrieb. Für die eingesetzte Software und Hardware bestehen Wartungsverträge mit den jeweiligen Lieferanten, die eine kurzfristige Verfügbarkeit der Systeme nach Störungen gewährleisten.

Regelung des Gebrauchs

Die Zugangsberechtigungen erlauben nur den Mitarbeiter der Abteilung Betrieb (Systemadministratoren) Veränderungen auf Systemebene durchzuführen. Bei Eingriffen mit höherem Ausführungsrisiko wird das 4-Augen Prinzip angewendet.

Wenn Systeme außer Betrieb genommen werden, werden die Informationen auf den Festplatten gelöscht. Die Festplatten werden vor der Verschrottung mechanisch zerstört. Somit wird sichergestellt, dass durch die Ausmusterung von Systemen keine Informationen kompromittiert werden.

Kennzeichnung der Systeme / Informationsklassifizierung

Alle Systeme erfüllen einen definierten Zweck. Deshalb stehen ihnen in der Prozesskette für ihre Aufgaben auch nur bestimmte Informationen zur Verfügung, die von diesen Systemen verarbeitet werden. Die Systeme sind dokumentiert und mit einem eindeutigen Systemnamen versehen.

Geregelte und sichere Handhabung von Werten

Die Betreuung aller im Rechenzentrum installierten Systeme liegt ausschließlich in der Verantwortlichkeit der Mitarbeiter der Abteilung Betrieb. Alle Zugriffe außerhalb der normalen Programmverarbeitung werden von der Abteilung Betrieb gesteuert. Die Funktionsfähigkeit der Systeme wird regelmäßig durch Testläufe überprüft und entsprechend dokumentiert.

Gesicherte Handhabung von Wechseldatenträgern

Zur Durchführung der Auslagerung von Datensicherungen werden Wechseldatenträger verwendet. Die Datensicherung unterliegt einem festgelegten

dokumentierten Sicherungsschema. Die Mitarbeiter des Operating entnehmen den Bandrobotern der Sicherungssysteme die Datenträger nach einem festgelegten Datenträgerentnahme- und -zuführungsplan. Dabei werden die Datenträger ohne Zwischenlagerung unmittelbar in die für die Datensicherung zugewiesenen Datensicherungstresore verbracht. Den ausführenden Mitarbeitern ist die Brisanz dieser Tätigkeit unter dem Aspekt des Schutzes der Daten transparent.

Entsorgung von Datenträgern

Die Entsorgung von Datenträgern erfolgt kontrolliert unter Einbindung zertifizierter Entsorgungsdienstleister. Jede Vernichtung wird dokumentiert und mit einem Zertifikat für die datenschutzrechtlich ordnungsgemäße Entsorgung verbunden.

Maßnahmen zur Instandhaltung von Systemen

Analyse und Spezifikation von Sicherheitsanforderungen

Bei der Entwicklung von Anwendungen werden Sicherheitsaspekte beleuchtet und technisch bei der Programmierung berücksichtigt. Die Betriebssysteme werden regelmäßig aktualisiert. Von einer externen Firma werden Pentests durchgeführt, um die in der Entwicklung umgesetzten Sicherheitskonzepte auch auf die tatsächlich erreichte Sicherheit hin zu kontrollieren.

Sicherung von Anwendungen in öffentlichen Netzen

Alle von raw angebotenen Dienste werden über gesicherte Protokolle wie https, sftp, ssh, AS2 oder einen dedizierten VPN-Tunnel verschlüsselt angeboten. Dadurch wird sichergestellt, dass keine Verbindungen kompromittiert werden können. Die dafür erforderlichen öffentlichen Zertifikate werden regelmäßig erneuert, da ihre Laufzeit begrenzt ist.

Überprüfung von Anwendungen nach Änderungen am Betriebssystem

Hier unterscheiden wir zwei Stufen von Änderungen:

- Sicherheitsupdates und Systemupdates
- Releaseupdates

Bei Sicherheitsupdates und Releaseupdates werden keine nachträglichen Anwendungstests durchgeführt. Veränderungen am Betriebssystem können in diesem Umfeld wieder zurückgenommen werden.

Bei einem Releaseupdate wird das System komplett neu aufgebaut und ein gesamter Systemtest mit allen Komponenten durchgeführt.

Wir setzen für automatisierte Tests einen Bamboo-Server von der Fa. Atlassian ein. Hierüber wird sichergestellt, dass die Tests immer alle gewünschten Parameter berücksichtigen. Für Neu- bzw. Weiterentwicklungen werden die Tests ständig erweitert. Die Tests unterliegen einer Zugriffsberechtigungsstruktur.