Vertrauensdienstrichtlinie
bitkasten eIDAS Zustellung – Qualified Electronic Delivery Service (QERDS)

bitkasten – Mit Sicherheit nachhaltig kommunizieren!

Datum: Juli 2024
Version: 1.1

Dokumentenhistorie

Version	Änderung	Datum
1.1	Änderung der Rechtsgrundlage auf Grund der Neuerlassung der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität	08.05.2024
1.0	Erstellung im Rahmen der Zertifizierung der eIDAS-Konformität als QERDS	15.04.2024

Inhaltsverzeichnis

***Hinweis**: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.*

Einführung

Dieses Dokument ist als Vertrauensdienstrichtlinie (engl. Trust Service Practice Statement, TSPS) der bitkasten GmbH zu verstehen, einem Anbieter von Vertrauensdiensten (engl. Trust Service Provider, TSP). Diese Richtlinie regelt speziell den Dienst *bitkasten eIDAS Zustellung* für die Übermittlung elektronischer Einschreiben und Dokumente gemäß Artikel 3 Nr. 16 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 (nachfolgend: eIDAS-Verordnung). Die eIDAS-Verordnung betrifft elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und hebt die Richtlinie 1999/93/EG auf. Sie legt die Regeln für elektronische Identifikationen und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt fest.

Das TSPS der bitkasten GmbH gilt exklusiv für den Service der Zustellung elektronischer Einschreiben, der sowohl für natürliche Personen als auch für juristische Entitäten über den Vertrauensdienst *bitkasten eIDAS Zustellung* abgewickelt wird.

Zertifizierung der eIDAS-Konformität als QERDS

QERDS (Qualified Electronic Registered Delivery Service) ist ein elektronischer Einschreibezustellungsdienst, der den Anforderungen der europäischen Verordnung (EU) 2024/1183, Artikel 44 entspricht.

Durch die Zertifizierung der eIDAS-Konformität als QERDS ermöglicht die *bitkasten eIDAS Zustellung* das Senden elektronischer Dokumente an Empfänger inklusive Sicherung der Nachweise für die Zustellung für sieben Jahre.

Unser Dienst ist speziell darauf ausgerichtet, Unternehmen, Behörden und öffentlichen Einrichtungen einen vertrauenswürdigen Weg für den Versand elektronischer Dokumente zu bieten. Wir garantieren durch fortgeschrittene Sicherheitstechnologien und genaue Protokollierung der Versand- und Empfangszeiten nicht nur die Authentizität der Dokumente, sondern auch deren Integrität durch Schutz vor Verlust, Diebstahl, Beschädigung oder unbefugten Änderungen während der Zustellung.

Überblick

Die bitkasten GmbH ist ein deutscher Software-as-a-Service (SaaS) und Green Tech-Anbieter für die vollständige Digitalisierung der Briefkommunikation und des Informationsaustauschs. Die Lösung ist der bitkasten, eine Digitalisierungs- und Kommunikationsplattform – ökologisch, nachhaltig und smart.

Mit dem bitkasten überbrücken Unternehmen und Kommunen die „letzte Meile" zu Kunden, Mitarbeitenden und Bürgern durch die Digitalisierung der Input- und Output-Prozesse. Dies erfolgt ohne aufwändiges IT-Projekt innerhalb kurzer Zeit durch Verwendung bestehender Druckdaten und bekannter Postadressen. Die nachhaltige digitale Briefkommunikation führt zu einer Reduzierung der Druck, Porto- und Prozesskosten.

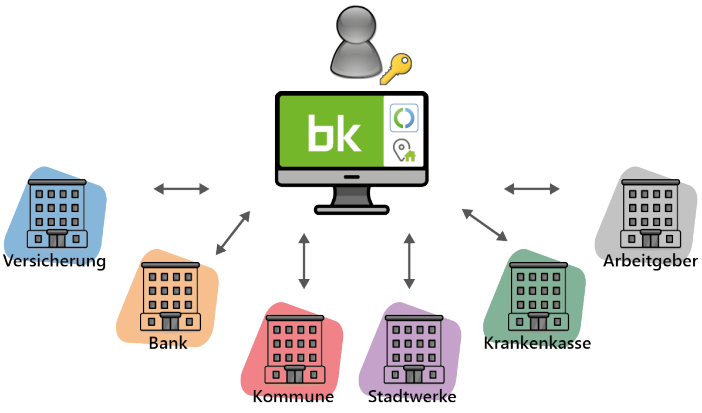
Der bitkasten empfängt Post digital von allen teilnehmenden Absendern. Die Briefe gehen rechtssicher an den digitalen, smarten Briefkasten zu und gelten als zugestellt, sobald Empfänger diese Öffnen oder Herunterladen. Der bitkasten steht für schnelle Kommunikation wie E-Mail, aber ohne E-Mail-Adresse, dafür sicher und DSGVO-konform. Die Identifizierung und digitale Zustellung der Kommunikation erfolgen mittels der bekannten Postadresse über den elektronischen Personalausweis. Für Empfänger funktioniert die Kommunikation im bitkasten ohne Medienbruch via App oder Web.

Fakten im Überblick

- Ein digitaler Briefkasten, der mehr ist als nur ein Postfach: Kommunikation mit Adressaten
- Zugriff auf den digitalen Briefkasten über kostenlose App oder im Web
- Zustellung und Identifizierung über Postadresse
- Nachhaltige Briefkommunikation ohne Druck und physikalische Zustellung
- Einführung fast ohne IT-Projekt und Anpassung von Systemen sowie Dokumenten
- bitkasten als Basis für die Abbildung weiterer papierbezogener Prozesse
- DSGVO-konform: Kein E-Mail Spam, keine Weitergabe persönlicher Daten

bitkasten Prinzip

Den bitkasten kann man mit dem Briefkasten an der Hauswand vergleichen – nur eben digital. In den Briefkasten erhalten Empfänger adressierte Post, wie beispielsweise die des Arbeitgebers, der Versicherung etc. Der digitale Briefkasten funktioniert nicht anders – nur, dass Empfänger Post von den Absendern digital im bitkasten finden. Dabei empfängt und archiviert der bitkasten digitale Post von allen teilnehmenden Absendern.



Leistungsumfang für Absender

Identifizierung der juristischen Person

Absender sind Unternehmen oder Einrichtungen, die an identifizierte Personen digital Post senden.

Bei der Identifizierung von Absendern – also juristischer Personen – setzen wir auf das Extended Validation SSL Zertifikat (EV SSL), dessen Ausgabe an strengere Vergabekriterien gebunden ist. Dies bezieht sich vor allem auf eine detaillierte Überprüfung des Antragstellers durch die Zertifizierungsstelle. Bei der Authentifizierung wird festgestellt, ob es sich bei der juristischen Person auch wirklich um das Unternehmen handelt, was es vorgibt zu sein. Dabei wird die Echtheit der Identität mithilfe digitaler Zertifikate belegt.

Digitale Dokumentenzustellung

Zugriffskontrolle

Nach der Identifizierung und Authentifizierung der gesetzlichen Vertreter der juristischen Person (Absender) kann die Übertragung der Dokumente an bitkasten erfolgen. Dabei liegt die Verantwortung der Zugriffskontrolle bzw. des Rollenmanagements beim Absender selbst.

Dokumentenaufbereitung

Bei der Übertragung von Dokumenten vom Absender bis hin zur Zustellung dieser an den Empfänger stellen wir die Unversehrtheit bzw. Unveränderbarkeit der Dokumente sicher.

Bereitstellung von Dokumenten

Der Informationsaustausch im bitkasten funktioniert grundsätzlich rein digital. Er beginnt mit der Bereitstellung der Dokumente durch den Absender.

Digitale Zustellung

Die Identifizierung und digitale Zustellung an Empfänger erfolgen mittels der bekannten Postadresse. Dank der bestätigten Identität und der festgestellten Anschrift ist sichergestellt, dass die Zustellung korrekt ist. Die Anschrift kann von Empfängern nicht selbständig geändert werden.

Übernahme der Verantwortung

Die Übertragung eines digitalen Dokuments als elektronisches Einschreiben bzw. eIDAS Dokument beginnt mit der Einlieferung durch den Absender. Die bitkasten GmbH übernimmt die Verantwortung der Zustellung, wenn das System ermittelt hat, dass es einen Empfänger gibt und die Adressdaten übereinstimmen.

Zustellungs- und Empfangsbestätigung

Die *„bitkasten eIDAS Zustellung"* liefert Nachweise über Ereignisse, die während der Übertragung von Dokumenten zwischen den Parteien stattfinden (zum Beispiel Informationen, dass die Daten vom Absender gesendet oder beim Empfänger zugestellt wurden). Diese können gegenüber Dritten und auch in Gerichtsverfahren verwendet werden, um den Austausch von Informationen bzw. Dokumenten zu einem bestimmten Zeitpunkt zu belegen. Der Zeitpunkt und die Unversehrtheit wird durch qualifizierte Siegel und qualifizierte Zeitstempel bestätigt.

Dokumentenempfang für Empfänger

Identifizierung

Empfänger im bitkasten sind natürliche Personen, die Dokumente von Absendern digital erhalten.

Sie können sich kostenfrei für den persönlichen digitalen Briefkasten (bitkasten) registrieren. Hierzu erfolgt einmalig eine Identifizierung. Um es Empfängern so einfach wie möglich zu machen, haben wir verschiedene Identifizierungsverfahren implementiert. Im Verlauf der Registrierung wird zudem die Handynummer mittels Authentifizierungsmittel mit dem Konto verknüpft.

Registrierung mit IDnow

Dieses Registrierungsverfahren ermöglicht Empfängern, sich schnell und unkompliziert zu identifizieren. Dabei können sie ihre Identität mittels biometrischer Merkmale und Dokumentenscan einfach über ihr Smartphone bestätigen.

Registrierung mit eID Funktion des deutschen Personalausweises oder Aufenthaltstitels

Empfänger können die Identität mit dem Ausweisdokument und dem dazugehörigen PIN eindeutig bestätigen. Alles, was dafür benötigt wird:

- Deutscher Personalausweis oder Aufenthaltstitel mit aktivierter eID-Funktion
- Passender Kartenleser (z.B. Smartphone mit NFC Funktion)
- Installierte AusweisApp (kostenfrei in allen Appstores verfügbar)

Login bitkasten & Authentifizierung

Empfänger können sich mit den persönlichen Zugangsdaten im bitkasten anmelden. Dies kann über den Webbrowser oder per App (iOS, Android) erfolgen. Sie haben Zugriff auf die für sie bereitgestellten Dokumente, das persönliche Archiv und auf die vom Absender bereitgestellten Services. Für zusätzliche Sicherheit kann eine 2-Faktor-Authentifizierung oder biometrische Anmeldung aktiviert werden.

Eine *bitkasten eIDAS Zustellung* ist durch ein Symbol visuell erkennbar. Bevor das Dokument geöffnet werden kann, muss der Empfänger sich authentifizieren, um sicherzustellen, dass nur dieser Zugang zu diesem Dokument erhält.

Rechtssicherer Zustellnachweis

Information zur Beweiserzeugung

Wir sammeln und speichern im Rahmen der *bitkasten eIDAS Zustellung* Daten über:

- Alle Ereignisse, die mit der anfänglichen Überprüfung der Identität des Absenders und dessen Identifizierung zusammenhängen
- Alle Ereignisse, die mit der anfänglichen Überprüfung der Identität des Empfängers und dessen Identifizierung zusammenhängen
- Bei der anfänglichen Überprüfung der Identität werden die Ausweisdaten einer natürlichen Person (z.B. Personalausweis), die Identifikationsdaten einer juristischen Person (gültiges EV SSL Zertifikat) und alle anderen Daten, die für ihre korrekte Feststellung notwendig sind, überprüft
- Daten, die für die anfängliche Identifikation des Absenders/Empfängers bestimmt sind
- Nachweise, dass der Absender vor Sendungsübergabe ordnungsgemäß authentifiziert wurde
- Nachweise, dass das Dokument vom Empfänger erhalten wurde
- Nachweise, dass das Dokument während der Übertragung nicht verändert wurde

Archivierung von Ereignissen und Nachweisen

Alle Dokumente und Daten, die im Identitätsüberprüfungsprozess verwendet werden, unterliegen der Archivierung. Die Informationen nach Art. 24 Absatz 2 Buchstabe h) der Verordnung (EU) 2024/1183 (alle relevanten Informationen in Bezug auf von der bitkasten GmbH ausgestellte und empfangene Daten, insbesondere im Hinblick auf die Beweisführung in Gerichtsverfahren und die Sicherstellung der Kontinuität bei der Diensterbringung) werden für einen Zeitraum von mindestens sieben Jahren gespeichert. Die Speicherung erfolgt auch nach Beendigung der Tätigkeit der bitkasten GmbH.

Die langfristige Datenspeicherung erfolgt an einem sicheren und geschützten Ort. Die spezifischen Bedingungen entsprechen den geltenden Standards, Empfehlungen und Vorschriften im Bereich der Informationssicherheit. Daten werden in einer Weise gesammelt, die mit der Art des Dokuments übereinstimmt. Der Zugang zu den langfristig gespeicherten Daten ist nur autorisierten Personen gestattet.

Betriebszeiten und Kundensupport

Im Folgenden sind wichtige Informationen zur Verfügbarkeit unserer bitkasten-Plattform sowie zu den Servicezeiten unseres Kundendienstes aufgeführt. Diese decken sowohl die Seite des Absenders als auch Empfängers ab.

Verfügbarkeit

Die bitkasten-Plattform und die damit verbundene *bitkasten eIDAS Zustellung* sind rund um die Uhr (24/7) für den Absender und Empfänger verfügbar, außer in Fällen von:

- Geplanten und vorab angekündigten Wartungsarbeiten an der Infrastruktur.
- Ungeplanten Wartungsarbeiten an der Infrastruktur als Ergebnis von unvorhergesehenen Ausfällen.
- Wartung aufgrund von Infrastrukturausfällen, die nicht im Zuständigkeitsbereich des Anbieters liegen.
- Nichtverfügbarkeit des Dienstes als Ergebnis von höherer Gewalt oder außergewöhnlichen Ereignissen.

Geplante Wartung oder Aufrüstung der Infrastruktur wird mindestens drei Tage vor Beginn angekündigt. Soweit eine technische Störung vorhanden ist, werden wir diese Störung unverzüglich beseitigen.

Kundenservice

Unser Kundenservice steht Absendern telefonisch Montag bis Freitag von 08:30 – 17:30 Uhr (ausgenommen bundeseinheitliche Feiertage), per E-Mail oder über unser Kundenserviceformular auf der Webseite www.bitkasten.de/kundenservice zur Verfügung.

Unser Kundensupport für Empfänger ist telefonisch Montag bis Freitag von 09:00 – 17:00 Uhr (ausgenommen bundeseinheitliche Feiertage) verfügbar. Zudem ist das Team per E-Mail oder über unser Supportformular auf der Webseite www.bitkasten.de/support Verfügung. Auch haben wir FAQs auf unserer Webseite, die die häufigsten Fragen abdecken.

Datensicherheit und Datenschutz

Wir setzen auf Qualität, Sicherheit und Service. Durch die Einhaltung verschiedenster Richtlinien und Anforderungen stellen wir sicher, dass die Compliance Vorgaben der Absender erfüllt werden. Eine DSGVO-konforme Speicherung personenbezogener Daten und Informationen unserer bitkasten Nutzer ist für uns selbstverständlich. Entsprechend unserer Werte geben wir uns mit dem Status quo nicht zufrieden. Wir streben nach kontinuierlicher Verbesserung, hoher Kundenzufriedenheit und Qualität.

Grundlage von erfolgreichem Datenschutz ist eine gelebte Datenschutz-Kultur im gesamten Unternehmen und bei allen Lieferanten. Diese Kultur basiert sowohl auf dem richtigen Handeln im Umgang mit personenbezogenen Daten als auch darauf, neue Lösungen und Funktionen direkt mit dem Fokus der Einhaltung des Datenschutzes und – damit verbunden – der IT-Sicherheit zu planen und zu entwickeln. Beides sind u.a. architektonische Grundpfeiler auf denen der bitkasten entwickelt wurde.

Cyberangriffe haben in den kommenden Jahren verstärkt zugenommen. 67% der Angriffe in Deutschland im Jahr 2021 erfolgten durch Malware, Phishing und Ransomware, die über E-Mail verbreitet werden [1]. Durch den Verzicht von E-Mail adressiert der bitkasten diese Sicherheitsprobleme und minimiert die Risiken. Der bitkasten sorgt für eine sichere, digitale Vernetzung der Kommunikationspartner. Durch verschlüsselte Transportwege und einem eindeutig identifizierten Nutzerkreis stellen wir eine DSGVO-konforme Dokumentenzustellung sicher.

[1] Quelle: Bitkom

Neben der Identifizierung und Authentifizierung bilden eine Reihe von Sicherheitsmaßnahmen das Fundament für sichere, medienbruchfreie Kommunikation und Informationsaustauch.

Sicherheit					
DSGVO-konform	Ende-zu-Ende verschlüsselt	Keine E-Mail Zustellung	Schutz vor SPAM, Ransomware, Phishing	Einfache IT-Integrierbarkeit	
	Kein Opt-In notwendig	Keine kanalspezifische Aufbereitung	Schutz gegen Identity Fraud	Integriertes Empfängerarchiv	

Gemäß den Vorgaben aus der DSGVO und den auf die bitkasten GmbH ausgelegten Prozessen beinhaltet unser Datenschutzmanagementsystem die nachfolgenden Komponenten:

- Verzeichnis von Verarbeitungstätigkeiten: Beschreibung aller Verarbeitungen von personenbezogenen Daten nach Vorgaben Art. 30 DSGVO
- Auftragsverarbeitungsvertrag (AVV), Nutzungsbedingungen, Datenschutzrichtlinien: Definition Umgang mit personenbezogenen Daten
- Technische und organisatorische Maßnahmen: Definition implementierter Maßnahmen zur Wahrung der Datensicherheit
- Aufbewahrungs-, Lösch- und Notfallkonzepte Prozesse zum Umgang mit Daten
- Prozesse zur Einhaltung von Betroffenenrechten

Grundlagen unserer Datenschutzstrukturen und -prozesse bilden, die in Artikel 5 DSGVO beschriebenen sieben Grundprinzipien der Datenverarbeitung, an denen wir uns orientieren.

1. Rechtmäßigkeit: Ausschließliche Verarbeitung, der aktiv zur Verfügung gestellt Daten. Transparente und vollumfängliche Information über die Verwendung erhobener Daten.
2. Zweckbindung: Verarbeitung der erhobenen Daten ausschließlich für die Nutzung des bitkasten. Keine Datenweitergabe an Dritte, außer im Rahmen eines AVVs an Subunternehmer.
3. Datenminimierung: Erhebung ausschließlich von Pflichtdaten für die Nutzung des bitkasten (Vorname, Nachname, Adresse oder Personalnummer).
4. Richtigkeit: Sofortige Änderung von Bestandsdaten bei Aktualisierungsanfragen. Löschanfragen werden umgehend durchgeführt.
5. Speicherbegrenzung: Regelmäßiges Löschen von nicht mehr benötigte Daten.
6. Integrität und Vertraulichkeit: Zugriff auf Daten im bitkasten nur durch Nutzer selbst sowie vier geschulte Administratoren der bitkasten GmbH. Keine Datenweitergabe an Dritte.
7. Rechenschaftspflicht: Befolgter Grundsatz.

Wir gewährleisten absolute Verschwiegenheit und Geheimhaltung aller gewonnenen Informationen. Unsere Datenschutzbestimmungen sind unter www.bitkasten.de/datenschutzerklaerung zu finden.

Allgemeine Bestimmungen

Vertragsbedingungen

Die Verpflichtungen und Verantwortlichkeiten von Absendern und der bitkasten GmbH werden durch vertragliche Vereinbarungen sowie unseren Allgemeinen Geschäftsbedingungen geregelt. Die Verträge zur Bereitstellung der *bitkasten eIDAS Zustellung* werden unter Beachtung der Bestimmungen der Verordnung (EU) 2024/1183, des Vertrauensdienstegesetzes (VDG) und der Vertrauensdiensteverordnung (VDV) abgeschlossen.

Unsere Allgemeinen Geschäftsbedingungen sind unter www.bitkasten.de/agb zu finden.

Die Rechte und Pflichten von Empfängern werden vertragliche in den Nutzungsbedingungen und Datenschutzinformationen geregelt. Zur Nutzung des Dienstes müssen Empfänger während der Registrierung die Kenntnisnahme und Einhaltung dieser bestätigen.

Unsere Nutzungsbedingungen sind unter www.bitkasten.de/nutzungsbedingungen und die Datenschutzinformationen unter www.bitkasten.de/datenschutzinformationen zu finden.

Pflichten und Verantwortlichkeiten der bitkasten GmbH

Wir stellen sicher, dass unsere Dienstleistung der *bitkasten eIDAS Zustellung* unter Einhaltung folgender Bedingungen durchgeführt wird:

- Die Bedingungen und Konditionen der Verträge und Nutzungsbedingungen, die Anforderungen der Verordnung (EU) 2024/1183 sowie die nationale Gesetzgebung werden eingehalten.
- Die bereitgestellte *bitkasten eIDAS Zustellung* wird so angeboten, dass keine Urheberrechte oder lizenzierten Rechte Dritter verletzt werden.
- Es werden ausschließlich Technologien verwendet, die die Systemzuverlässigkeit sowie die technische und kryptographische Sicherheit bei der Durchführung der Prozesse sicherstellen.
- Informationen im Zusammenhang mit der *bitkasten eIDAS Zustellung* und der Betriebsleistung der Systeme werden sicher gespeichert und gepflegt.
- Die erforderlichen Betriebsverfahren sowie die technischen und physischen Kontrollvorschriften werden eingehalten.
- Es wird sichergestellt, dass eine genaue Zeitbestimmung des Sendens und Empfangens der Dokumente erfolgt.
- Identifikations- und Authentifizierungsverfahren werden für natürliche und juristische Personen oder für bevollmächtigte Vertreter juristischer Personen durchgeführt.
- Bei technischen Sicherheitsproblemen werden unverzüglich Maßnahmen ergriffen.
- Kunden werden über ihre Verpflichtungen und die gebotene Sorgfalt bei der Nutzung informiert.

- Die gesammelten persönlichen und sonstigen Informationen werden nur für den Zweck der Erstellung eines bitkasten Accounts sowie der Übertragung und Zustellung von Dokumenten in den digitalen bitkasten verwendet und in Übereinstimmung mit der nationalen Gesetzgebung gespeichert.
- Eine Haftpflichtversicherung mit der erforderlichen Deckungsvorsorge gemäß Artikel 24 Absatz 2 Buchstabe c der Verordnung (EU) 2024/1183 ist für die Dauer der Aktivitäten abgeschlossen.
- Es wird zuverlässiges Personal beschäftigt, das über die nötige Expertise, Erfahrung und Qualifikationen verfügt.
- Periodische interne Audits sowie externe Audits durch unabhängige Prüfer werden durchgeführt.

Datensparsamkeit

In Übereinstimmung mit den Grundsätzen der Datensparsamkeit und Datenvermeidung, wie sie in der Datenschutz-Grundverordnung (DSGVO) festgelegt sind, verpflichtet sich die bitkasten GmbH dazu, nur solche personenbezogenen Daten zu erheben und zu verarbeiten, die für die bereitgestellten Dienste zwingend erforderlich sind. Dies bedeutet, dass wir die Datenverarbeitungspraktiken stets daraufhin überprüfen und optimieren, um den Umfang der gesammelten Daten auf das absolut notwendige Minimum zu beschränken. Hierbei achten wir darauf, dass die Datenverarbeitung mit dem Zweck der Dienstleistung in Einklang steht und keine unnötigen oder übermäßigen Informationen von unseren Empfängern eingefordert werden. Durch diesen Ansatz gewährleisten wir einen verantwortungsvollen Umgang mit personenbezogenen Daten und fördern gleichzeitig den Schutz der Privatsphäre.

Pflichten des Absenders

Absender als Kunden der *bitkasten eIDAS Zustellung* haben folgende Pflichten:

- Sie müssen sich mit den Bedingungen des Vertrags, den AGB sowie der Leistungsbeschreibung vertraut machen und diese einhalten.
- Sie dürfen den zertifizierten QERDS *bitkasten eIDAS Zustellung* nur zu legitimen Zwecken nutzen.
- Sie müssen den im Vertrag mit bitkasten festgelegten Bedingungen und Konditionen zustimmen.
- Für die Verwendung der *bitkasten eIDAS Zustellung* ist eine Identifizierung der juristischen Person sowie der natürlichen Person als Vertreter notwendig.

Pflichten des Empfängers

Empfänger von *bitkasten eIDAS Zustellung* haben folgende Pflichten:

- Sie müssen sich mit den Nutzungsbedingungen und Datenschutzinformationen vertraut machen und diesen zustimmen.
- Sie dürfen den zertifizierten QERDS *bitkasten eIDAS Zustellung* nur zu legitimen Zwecken nutzen.
- Für das Öffnen und Lesen von *bitkasten eIDAS Zustellung* ist eine Authentifizierung notwendig.

Rechtswirkungen der angebotenen Vertrauensdienste

Art. 43 Absatz 1 eIDAS-Verordnung bestimmt zunächst, dass den Daten, die die Zustellung eines elektronischen Einschreibens bestätigen, Rechtswirkung zukommt und dass sie als Beweismittel vor Gericht verwendet werden dürfen.

Sofern die Dokumente mittels eines qualifizierten Dienstes für die Zustellung elektronischer Einschreiben wie dem bitkasten abgesendet und empfangen werden, legt Art. 43 Absatz 2 eIDAS-Verordnung eine gesetzliche Vermutung fest. Die Vermutung gilt:

- der Unversehrtheit der Daten,
- der Absendung dieser Daten durch den identifizierten Absender,
- des Empfangs der Daten durch den identifizierten Empfänger,
- der Korrektheit des Datums und der Uhrzeit der Absendung und des Empfangs.

Ergänzend weisen wir darauf hin, dass eine ggfls. verwendete qualifizierte elektronische Signatur die gleiche Rechtswirkung wie eine händische Unterschrift hat (Art. 25 Absatz 2 eIDAS-Verordnung).

Informationsverbreitung und Verantwortung

Die Informationen über den qualifizierten Vertrauensdienst, der von der bitkasten GmbH bereitgestellt wird, werden allen Interessenten auf der Unternehmenswebseite zur Verfügung gestellt.

www.bitkasten.de/eidas-rechtssichere-digitale-zustellung

Die vorliegende Vertrauensdienstrichtlinie unterliegt der Verantwortung und Verwaltung der bitkasten GmbH. Sie wurde von der Geschäftsführung genehmigt und regelmäßig aktualisiert. Alle Änderungen führen zu einer Veröffentlich der überarbeiteten Version.

bitkasten GmbH
Wallensteinstraße 63
90431 Nürnberg
www.bitkasten.de

Kontakt
0911 | 6000 2874
E-Mail: info@bitkasten.de

Übertragung von Aufgaben an Dritte

Auf der Grundlage und Maßgabe einer vertraglichen Vereinbarung erfolgt die Übertragung von Aufgaben und Pflichten an Dritte. Die bitkasten GmbH hat bei der Vertragsgestaltung gewährleistet, dass die aus der jeweiligen Aufgabenübertragung resultierenden gesetzlichen Anforderungen und die Regelungen der Vertrauensrichtlinie eingehalten werden. Die Verträge mit Drittparteien enthalten zudem die Verpflichtung zur Mitwirkung im Falle von internen und externen Audits, sowie dem Einräumen von Kontrollbesuchen der zuständigen Aufsichtsbehörde.

Die bitkasten GmbH hat in den folgenden Bereichen Aufgaben an Dritte übertragen:

- **Identdienstleister (IDnow GmbH):** Anbieter der eIDAS konformen Identitätsfeststellung natürlicher Personen. Berechtigt zur Identitätsfeststellung natürlicher Personen für Trust Service Provider (TSP) durch Konformitätsbestätigung nach eIDAS.
- **Rechenzentrumsbetrieb (Hetzner Online GmbH):** Hosting und Internet-Konnektivität werden von der Hetzner erbracht. Der Hostinganbieter ist zur Aufrechterhaltung seiner Zertifizierung nach ISO/IEC 27001 verpflichtet.
- **mTAN-Absender (Brevo)**: Brevo ist eine eingetragene Marke der Sendinblue GmbH. Anbieter von transaktionalen SMS, mit denen wir Einmalpasswörter für die Authentifizierung der Teilnehmer zustellen.
- **eID-Servicebetreiber (D-Trust GmbH & Bundesdruckerei):** Diese stellt Server-Komponenten zur Verfügung, um Identifizierungen mittels elektronischer Identitäten sicherzustellen. Die Ausweisapp wird bereitgestellt von Governikus.
- **Fernsiegeldienst (D-Trust GmbH):** Fernsiegeldienst stellt qualifizierte Siegel und Zeitstempel aus.

Die Gesamtverantwortung für den Betrieb des Vertrauensdienstes *bitkasten eIDAS Zustellung* verbleibt auch bei der Übertragung von Aufgaben an Drittparteien in der Hand der bitkasten GmbH. Alle Unternehmen wurden zur Einhaltung der rechtlichen Anforderungen verpflichtet. Die Umsetzung der Maßnahmen wird in regelmäßigen Abständen überprüft.

Bauliche und organisatorische Maßnahmen

Die bitkasten GmbH hat bauliche und organisatorische Maßnahmen umgesetzt, um den gesetzlichen Vorgaben zu entsprechen. Die Infrastruktur zur Leistungserbringung der *bitkasten eIDAS Zustellung* befindet sich in einem gesicherten Gebäude. Erfahrenes Personal der bitkasten GmbH ist für den Betrieb verantwortlich. Die Arbeitsprozesse des qualifizierten Zustelldienstes für elektronische Einschreiben sind präzise festgelegt.

Informationssicherheitsrichtlinien

Die Geschäftsführung der bitkasten GmbH hat Richtlinien für die Informationssicherheit sowie detailliertere Bestimmungen erlassen, die die Basisanforderungen für sämtliche IT-Systeme und IT-basierten Prozesse festlegen. Diese Vorschriften sind für alle angestellten Personen der bitkasten GmbH sowie für beauftragte Drittparteien verbindlich. In der bitkasten GmbH und im Rahmen der Leistungserbringung als *bitkasten eIDAS Zustellung* werden diese Richtlinien umgesetzt und gewahrt. Die Gesamtverantwortung für die Befolgung der in den Sicherheitsrichtlinien festgelegten Verfahren trägt die bitkasten GmbH. Sollten Drittparteien Teile der TSP-Funktionen übernehmen, sichert die bitkasten GmbH die Einhaltung der Sicherheitsstandards durch regelmäßige Audits ab. Im Informationssicherheitsmanagementsystem (ISMS) der bitkasten GmbH sind Maßnahmen festgehalten, die gewährleisten, dass das Sicherheitsniveau durch externe Dienstleistungen nicht kompromittiert wird. Von der Planung und Konzeption bis zum Betriebsende reichende Sicherheitsanforderungen wurden festgeschrieben, genehmigt und intern veröffentlicht.

Die Übereinstimmung von Drittparteien mit den Sicherheitsrichtlinien wird von der bitkasten GmbH durch Audits und/oder durch Zertifizierung gemäß ISO/IEC 27001 kontrolliert. Zusätzlich werden regelmäßige Überprüfungen basierend auf dem Zertifizierungsprozess durchgeführt. Änderungen an den Informationssicherheitsleitlinien werden Dritten, einschließlich Absendern und Empfängern, Dienstleistern, Bewertungsstellen und Aufsichtsbehörden, mitgeteilt, sofern dies notwendig ist.

Bauliche Sicherheitsmaßnahmen

Die Systeme und sensiblen Daten, die für den Betrieb des Trust Service Providers bitkasten GmbH kritisch sind, befinden sich in physisch gesicherten Sicherheitszonen. Zugangskontrollsysteme garantieren, dass nur befugtes Personal Zutritt erhält. Jeglicher Zutritt, einschließlich unautorisierter Versuche, wird aufgezeichnet. Sicherheitsverletzungen wie Einbrüche, Diebstahl oder Vandalismus setzen sofort Alarme in Gang. Die sicheren, hochverfügbaren und redundant ausgelegten Rechenzentren werden von der Hetzner Online GmbH verwaltet und sind nach ISO/IEC 27001 zertifiziert, was den aktuellen technischen Standard bestätigt. Die Beherrschung von Sicherheitsrisiken gemäß dem neuesten Stand der Technik wird durch die Zertifizierung gemäß ISO/IEC 27001 belegt.

Verfahrensvorschriften

Rollenkonzept

Im ISMS der bitkasten GmbH ist ein Rollenkonzept verankert, das operative, administrative und leitende Funktionen klar trennt, um den Grundsätzen der Funktionstrennung gerecht zu werden. Dieses Konzept beschränkt den Zugang zu IT-Systemen und Fachverfahren auf autorisiertes Personal. Rollen werden den angestellten Personen durch einen etablierten Prozess zugeteilt, basierend auf den für ihre Aufgaben erforderlichen Berechtigungen. Um sicherheitskritische Änderungen durch einzelne Individuen zu verhindern, wird ein Ausschlussprinzip angewendet. Der Prozess zum Entziehen von Rollen ist ebenso definiert und wird sorgfältig dokumentiert. Dem Rollenkonzept liegen die folgenden Basisregeln und Rollenausschlüsse zugrunde:

- Leitende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Administrative Rollen dürfen keine operativen Aufgaben übernehmen

Der Zugriff der Administratoren wird entsprechend eines Rollenkonzeptes geregelt und umfasst jeweils den Verantwortungs- bzw. Kompetenzbereich der Rolle und der zugehörigen Gruppe von Administratoren.

Vertrauenswürdige Rollen, wie z.B. Systemadministratoren und andere sind vollumfänglich etabliert und im ISMS dokumentiert. Die Rollen sind vom Management und dem Rolleninhaber akzeptiert und anerkannt.

Vier-Augen Prinzip

Sicherheitskritische Vorgänge erfolgen grundsätzlich im Vier-Augen-Prinzip. Dies wird durch technische und organisatorische Maßnahmen sichergestellt.

Sonstige Arbeitsanweisung

Den angestellten Personen der bitkasten GmbH ist es nicht erlaubt, Unterlagen, Medien (mit der Ausnahme von Laptops) und Software, die sensible Daten enthalten, aus dem Sicherheitsbereich der bitkasten GmbH zu entfernen.

Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Sicherheitsmaßnahmen des Vertrauensdienstes *bitkasten eIDAS Zustellung* beruhen auf einer detaillierten Risikoanalyse und sichern ein hohes Sicherheitsniveau. Diese Maßnahmen sind in im ISMS festgehalten, das intern bleibt und nicht öffentlich zugänglich ist. Das ISMS sowie die beschriebenen Sicherheitsvorkehrungen werden von der bitkasten GmbH kontinuierlich reevaluiert. Die Einhaltung aktueller technischer Sicherheitsstandards wird durch eine Zertifizierung nach DIN EN ISO/IEC 27001:2017 belegt.

Einige der organisatorischen Sicherheitsvorkehrungen umfassen:

- Im ISMS festgelegte Methoden zur Identifikation, Bewertung und regelmäßiger Kontrolle verbleibender Risiken.
- Sicherheitsrelevante Änderungen an den Systemen des Rechenzentrums unterliegen einer strengen Prüfung vor der Implementierung. Überwachungsbehörden werden über jegliche Modifikationen bei der Bereitstellung des qualifizierten Vertrauensdienstes sowie über die potenzielle Beendigung dieser Services informiert.
- Die strikte Befolgung des Artikels 24 (2a) der eIDAS-Verordnung wird gewährleistet.
- Alle sicherheitsrelevanten Verfahren sind im ISMS dokumentiert und überprüft.
- Die bitkasten GmbH hält Zertifikate für DIN EN ISO/IEC 27001:2017 und DIN EN ISO 9001:2015.

Die personellen Sicherheitsmaßnahmen, die von der bitkasten GmbH implementiert wurden, sorgen für ein hohes Sicherheitsniveau im Rahmen des Vertrauensdienstes *bitkasten eIDAS Zustellung*. Die angestellten Personen sind klar definierten Rollen innerhalb des Dienstes zugeordnet und werden entsprechend ihren Aufgaben geschult. Zudem erhalten sie alle erforderlichen Unterlagen, um ihre Tätigkeiten effizient auszuführen, und ihre Vertrauenswürdigkeit wird sorgfältig geprüft.

Das festgelegte ISMS der bitkasten GmbH umfasst detaillierte Rollenbeschreibungen und definiert die Trennung von Rollen bei kritischen Prozessen. Zur Unterstützung der täglichen Arbeit gibt es spezifische Arbeitsanweisungen.

Qualifikation, Erfahrung und Zuverlässigkeit des Personals

Die bitkasten GmbH verpflichtet sich, ausschließlich Personen einzustellen, die sowohl zuverlässig als auch qualifiziert sind. Vor dem Arbeitsantritt bei bitkasten GmbH wird die fachliche Kompetenz der angestellten Personen überprüft und Schulung basierend auf den Besonderheiten der Anforderungen an den Vertrauensdienst *bitkasten eIDAS Zustellung* durchgeführt. Dieses Verfahren wird auch auf Führungskräfte angewendet. Weiterbildungen und Schulungen werden systematisch dokumentiert. Die bitkasten GmbH legt darauf Wert, Interessenkonflikte zu vermeiden. Sollten solche Konflikte auftreten, ist es den angestellten Personen auferlegt, sich von der jeweiligen Tätigkeit zu distanzieren, ohne dass ihnen arbeitsrechtliche Nachteile entstehen.

Sicherheitsüberprüfung

Die bitkasten GmbH stellt sicher, dass das für den Vertrauensdienst *bitkasten eIDAS Zustellung* eingesetzte Personal die für einen sicheren Betrieb notwendige Zuverlässigkeit besitzt. Jede angestellte Person, der mit dem sicheren Betrieb betreut wird, muss bei Neueinstellung ein Führungszeugnis nach § 30 Abs. 1 und 5 des Bundeszentralregistergesetzes vorlegen.

Schulungen und Weiterbildungen

Jede angestellte Person der bitkasten GmbH wird vor Arbeitsantritt umfassend geschult und bei Bedarf fortgebildet. Die Schulungen umfassen eine gründliche Einführung in die zugewiesenen Aufgaben, eine Sensibilisierung für die Sicherheitsrelevanz der Tätigkeit sowie eine Unterrichtung über Datenschutzbestimmungen. Refresher-Kurse erfolgen routinemäßig in der Regel jährlich, mindestens jedoch alle zwei Jahre und zusätzlich bei Änderungen in den Abläufen, der verwendeten Technologie oder den betrieblichen Rahmenbedingungen, sofern diese für die Wahrung der Fachkompetenz notwendig sind. Die Inhalte der Schulungen werden fortlaufend auf ihre Aktualität hin überprüft.

Aktuelle Informationen zu Gefährdungen, Bedrohungen und Entwicklungen im Bereich der Informationssicherheit werden den angestellten Personen kontinuierlich vermittelt.

Rollenbesetzung, Rollenentzug und Rollenwechsel

Rollenbesetzungen, Rollenentzug und Rollenwechsel erfolgen nach festgelegten internen Verfahren. Eine Berufung erfolgt erst, wenn die erforderliche Sicherheitsprüfung und die erforderlichen Schulungen durchgeführt worden sind.

Sicherung und Aufzeichnungen

Die bitkasten GmbH richtet sich nach den rechtlichen Vorgaben für die elektronische Archivierung beim Betrieb einer Infrastruktur nach der eIDAS-Verordnung. Die sicher archivierten Daten umfassen u.a. Daten der Identifikation bzw. Authentifizierung einer natürlichen sowie juristischen Person, dokumentationspflichtige Vorgangsdaten wie Änderungsvorgänge, Sende- und Empfangsvorgänge, sowie Protokolle und andere Betriebsdaten, die durch den Dienst entstehen.

Wiederherstellung des Betriebes im Katastrophenfall

Die bitkasten GmbH verfügt über eine umfassende Notfalldokumentation und entsprechende Notfallpläne. Es gibt ein datenübergreifendes Backup-Konzept, um die Integrität und Wiederherstellbarkeit kritischer Daten zu sichern. Dabei werden regelmäßige Sicherungen der Datenbanken, Dateisysteme und der Konfigurationsdaten der IT-Systeme durchgeführt.

Es gibt einen allgemeinen Plan für den Systemneustart sowie Wiederanlauf, der sowohl das Gesamtsystem als auch die einzelnen Systemkomponenten und Dienste im Detail abdeckt. Im Rahmen des Management von Sicherheitsvorfällen (Incident Management) werden alle Störungen aufgenommen, bearbeitet und analysiert, inklusive einer Ursachenanalyse, um zukünftige ähnliche Zwischenfälle zu verhindern. Zur Unterstützung dieser Prozesse stehen ausreichend finanzielle Mittel sowie technische und personelle Ressourcen zur Verfügung.

Einstellung des Betriebes

Die bitkasten GmbH hält einen stets auf dem neuesten Stand gehaltenen Beendigungsplan bereit, der im Falle einer Geschäftsaufgabe greift, jedoch nicht öffentlich einsehbar ist. Dieser Plan, der die Schritte zur Betriebseinstellung detailliert beschreibt, wird in regelmäßigen Abständen von der zuständigen Behörde überprüft und genehmigt.

Im Falle einer geplanten Betriebseinstellung informiert die bitkasten GmbH die Teilnehmer und betroffene Dritte, einschließlich vertrauenswürdiger Drittparteien und Aufsichtsbehörden, rechtzeitig und möglichst mindestens drei Monate im Voraus, über die bevorstehende Einstellung und die daraus resultierenden Konsequenzen.

Verträge mit Dienstleistern sowie weitere Vertragsbindungen werden entsprechend der vertraglichen Fristen aufgelöst.

Obwohl die bitkasten GmbH bestrebt ist, den Vertrauensdienst durch einen anderen qualifizierten Trust Service Provider fortführen zu lassen, kann eine solche Übernahme nicht garantiert werden. Sollten Teilnehmerdaten an einen anderen qualifizierten TSP übergehen, bewahrt die bitkasten GmbH alle relevanten Informationen, bis bestätigt werden kann, dass diese vom übernehmenden TSP nicht mehr benötigt werden.

Falls kein anderer Dienstleister den Dienst übernimmt, ist die bitkasten GmbH verpflichtet, sicherzustellen, dass die gespeicherten Daten für einen Zeitraum von mindestens drei Monaten nach der Ankündigung der Geschäftsaufgabe zugänglich bleiben.

Asset Management

Die bitkasten GmbH gewährleistet ein adäquates Sicherheitsniveau für alle Unternehmenswerte, einschließlich der Informationsträger (Information Assets). Die Methoden zum Schutz dieser Informationsressourcen sind im ISMS festgelegt und durch eine Zertifizierung nach DIN EN ISO/IEC 27001:2017 bestätigt. Die genutzten IT-Systeme sind in einer Komponentenübersicht erfasst, wobei das entsprechende Sicherheitsniveau den gesetzlichen Anforderungen entspricht.

Technische Sicherheitsmaßnahmen

Die bitkasten GmbH errichtet ihre Infrastruktur mit mehrfach konfigurierten Systemen. Serverdienste sind so eingerichtet, dass sie ausschließlich erforderliche Hardwarekomponenten, wie Netzwerkschnittstellen, nutzen. Alle nicht notwendigen Software- und Hardwarekomponenten werden deaktiviert. Sicherheitsanforderungen werden bereits in der Planungsphase von neuen Systemaufbauten, Änderungen, Erweiterungen und Softwareentwicklungen berücksichtigt.

Eine regelmäßige, zentrale Datensicherung verhindert Datenverlust. Das Sicherheitsniveau der Server basiert auf dem Schutzbedürfnis der darauf gespeicherten Daten. Aufgrund der Natur der bei eIDAS-

Diensten verarbeiteten Daten ist grundsätzlich von einem hohen Bedarf zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit auszugehen.

Ein verbindlicher Prozess für Änderungen und Patch-Management sichert die zeitnahe und geordnete Implementierung von sicherheitsrelevanten Patches und Updates. Informationsquellen und Verfahren zur Identifikation und Behebung technischer Schwachstellen sind definiert.

Redundante Loadbalancer verteilen Anfragen auf die Serversysteme, die über mehrere Rechenzentren verteilt sind. Systeme zur Datenspeicherung werden repliziert und sind so konfiguriert, dass ein automatischer Wechsel zu redundanten Partnerkomponenten möglich ist. Zudem gibt es ein umfassendes Monitoring der Dienste, das rund um die Uhr läuft.

Für die Server gibt es ein Datensicherungskonzept und Notfallpläne für Ausfälle sowie für andere kritische Systeme. Störungen werden im Rahmen des Incident Managements bearbeitet. Regelmäßige Tests der Störungs- und Notfallverfahren sind geplant.

Netzwerktechnische Sicherheitsmaßnahmen

Die bitkasten GmbH betreibt ihre Infrastruktur in physisch und geografisch redundanten Rechenzentren, die durch redundante Systeme miteinander vernetzt sind, wobei der Datenaustausch zwischen diesen verschlüsselt erfolgt. Das Netzwerk ist in verschiedene Segmente unterteilt, um eine klare Netzwerksegmentierung zu gewährleisten. Die Kommunikation zwischen und innerhalb dieser Zonen wird durch Firewalls abgesichert. Das bestehende Regelwerk für die Firewalls wird regelmäßig überprüft und aktualisiert. Die Umgebungen für Produktion, Entwicklung und Testbetrieb sind strikt voneinander getrennt.

Ein fortlaufendes Monitoring-System überwacht die Komponenten und Betriebsparameter, indem ständig Leistungsmessungen und Analysen des Datenverkehrs durchgeführt werden. Bei Erreichen bestimmter Schwellenwerte oder beim Auftreten sicherheitsrelevanter Ereignisse werden umgehende Maßnahmen eingeleitet, wobei darauf geachtet wird, dass keine sensiblen Daten nach außen getragen werden.

Sicherheitsrelevante Vorgänge und Störungen sowie Zugriffe durch angestellte Personen werden lückenlos protokolliert. Dies umfasst insbesondere die Protokollierung von Start und Beendigung der IT-Systeme, der Logging-Funktionen, Systemabstürzen, Hardwareausfällen sowie Aktivitäten von Firewalls und Routern. Log-Dateien werden auf gesicherten gespeichert. Zugang zu diesen Daten haben ausschließlich befugte Personen.

Störungen im IT-Bereich werden durch klar definierte Verfahren geregelt. Der gesamte Prozess der Erkennung und Reaktion auf Störungen ist Teil des Incident Managements. Sowohl Hardware- oder Softwarestörungen, Angriffsversuche, Sicherheitsverstöße als auch Warnmeldungen des Monitoring-Systems werden den Administratoren gemeldet, die sofort mit der Fehlerbehebung oder der Eindämmung möglicher Sicherheitsereignisse beginnen. Sicherheitsrelevante Zwischenfälle und offene Sicherheitslücken werden umgehend an den Informationssicherheitsbeauftragten berichtet, der die notwendigen Maßnahmen zur Behebung des Vorfalls bewertet, deren Umsetzung veranlasst und die Vorfälle dokumentiert.

Backup- und Wiederherstellung

Das Hauptziel der bitkasten GmbH besteht darin, Datenverluste von Teilnehmerdaten unter allen Umständen zu verhindern. Aus diesem Grund sind die Rechenzentren über redundante Standorte verfügt, um höchste Verfügbarkeit und Ausfallsicherheit zu garantieren. Backup- und Wiederherstellungspläne sind detailliert ausgearbeitet und den zuständigen angestellten Personen vollständig bekannt. Um die Zuverlässigkeit dieser Pläne sicherzustellen, führt die bitkasten GmbH regelmäßig Tests zur Datenwiederherstellung durch.

Zugriffskontrolle

Die bitkasten GmbH gewährt den Zugang zu ihren IT-Systemen nur nach einer erfolgreichen Authentisierung. Nutzerrechte für den Zugriff auf Dateien und Programme sind streng nach dem Bedarfsprinzip ("Need-to-Know") geregelt und basieren auf den jeweiligen Rollen der Benutzer. Diese Rollen und die damit verbundenen Zugriffsrechte sind im ISMS dokumentiert. Zudem sind permanente oder unbeaufsichtigte Wartungszugänge durch externe Dienstleister ausgeschlossen, um die Sicherheit und Integrität der Systeme zu gewährleisten.

Incident Management

Ein Prozess zur Behandlung von Sicherheitsvorfällen als Bestandteil des Informationsmanagementsystem, welches nach DIN EN ISO/IEC 27001:2017 zertifiziert ist, wurde von der bitkasten GmbH implementiert. Dies hält den Betrieb des Vertrauensdienstes aufrecht und sichert ihn ab. Die angestellten Personen, die für die Überwachung verantwortlich sind, sind speziell qualifiziert, um die Systeme zu kontrollieren und auf Sicherheitsvorfälle schnell zu reagieren, was das frühzeitige Abwehren von Angriffen ermöglicht. Im Rahmen dieses Prozesses wird eine Ursachenanalyse durchgeführt, um wiederkehrende Störungen, die auf denselben Ursachen beruhen, zu verhindern.

Im Falle einer Sicherheitsverletzung oder eines Integritätsverlusts, der einen erheblichen Einfluss auf den Vertrauensdienst oder personenbezogene Daten haben könnte, informiert die bitkasten GmbH die entsprechenden Parteien gemäß den bestehenden Regulierungsvorschriften.

Es wird streng darauf geachtet, die Anforderungen des Artikels 19.2 der eIDAS-Verordnung vollständig zu erfüllen, und die zuständige Aufsichtsbehörde wird innerhalb von 24 Stunden über jeden wesentlichen Sicherheitsvorfall in Kenntnis gesetzt.

bitkasten GmbH
Wallensteinstraße 63
90431 Nürnberg
www.bitkasten.de

Kontakt
0911 | 6000 2874
E-Mail: info@bitkasten.de