



Technisch-organisatorische Maßnahmen

Anhang 1 zum Vertrag zur Auftragsverarbeitung

gemäß Artikel 32 Absatz 1 DS-GVO zum Stand 01.01.2022.



Public – Öffentlich

Disclosure is not limited.

Information may be distributed without restriction, including public release.

If you have questions regarding information classification, please contact:

infosec@aoe.com

Ansprechpartner

Datenschutzkoordinator

Daniel Wittich
AOE GmbH
Kirchgasse 6
65185 Wiesbaden
Tel.: +49 (6122) 70707 – 123
E-Mail: daniel.wittich@aoe.com

Datenschutzbeauftragter

Arndt Hallbach
GINDAT GmbH
Wetterauer Str. 6
42897 Remscheid
Tel.: +49 (2191) 909 – 437
E-Mail: datenschutz@aoe.com

Beschreibung der technisch-organisatorischen Maßnahmen

1. Gewährleistung der Vertraulichkeit der Systeme und Dienste

Maßnahmen, die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen.

1.1. Zutrittskontrolle

1.1.1. RFID Türkontrolle

Zutritt zu den Geschäftsräumen ist Mitarbeitern ausschließlich mit persönlich zugewiesenen RFID Schüsseln möglich. Schlüssel werden zu Beginn des Arbeitsverhältnisses protokolliert ausgegeben und nach Beendigung des Arbeitsverhältnisses umgehend zurückgefordert und deaktiviert.

1.1.2. Empfang und Wachdienst

Während der Kerngeschäftszeiten werden Besucher und Lieferanten durch das Empfangspersonal begrüßt, angemeldet und zu den jeweiligen Gastgebern bzw. Konferenzräumen eskortiert.

Außerhalb der Geschäftszeiten werden die Geschäftsräume regelmäßig durch einen Wachdienst kontrolliert.

Kontakt

Telefon +49 611 945 735 - 0
Fax +49 611 945 735 - 10
Mail info@bare.id
Web www.bare.id

Geschäftssitz

Bare.ID GmbH
Kirchgasse 6
65185 Wiesbaden
Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)
Registergericht Wiesbaden B HRB 33190

Bank

Wiesbadener Volksbank eG
Schillerplatz 4 | 65185 Wiesbaden
IBAN DE15 5109 0000 0005 2908 05
BIC/SWIFT WIBADE5W
Land Deutschland

1.1.3. Besucherregistrierung

Alle Besucher müssen sich bei Eintreffen in den Geschäftsräumen in einem elektronischen Besucherverzeichnis registrieren und eine Vertraulichkeitsvereinbarung sowie Verhaltensbestimmungen unterzeichnen.

1.1.4. Videoüberwachung

Außerhalb der Geschäftszeiten erfolgt eine Aufzeichnung der Videoüberwachung der Eingangsbereiche. Die Aufnahmen der Videoüberwachung werden 3 Tage vorgehalten.

1.1.5. Alarmanlage

Außerhalb der Geschäftszeiten sind die Geschäftsräume durch eine Alarmanlage gesichert. Nach Auslösung der Alarmanlage erfolgt ein Telefonrundruf in den Geschäftsräumen, wird dieser Rundruf nicht beantwortet oder durch einen Mitarbeiter mit Passwort quittiert, erfolgt ein kaskadierter Rundruf erst an bestimmte Mitarbeiter, den Wachdienst sowie die zuständige Polizeidienststelle.

1.1.6. Rechenzentrum

Der Zutritt zum Rechenzentrum ist nur nach vorheriger, namentlicher Anmeldung und einschlägiger Überprüfung der Personalien durch den Rechenzentrumsbetreiber möglich.

Zutritt durch Vereinzelungsanlagen zu verschlossenen Serverräumen nur für autorisiertes Personal.

Alarmierung bei nicht verschlossenen Türen.

1.2. Zugangskontrolle

1.2.1. Passwörter

Zugriff auf alle DV-Systeme ist erst möglich nach Authentifizierung und Autorisierung gegen das zentrale LDAP Verzeichnis.

Jeder Mitarbeiter erhält ausschließlich benannten Zugriff, generische Zugangsdaten werden nicht verwendet.

Passwörter müssen den folgenden Charakteristika entsprechen. Diese Bedingungen werden durch das LDAP Verzeichnis erzwungen.

- Mindestlänge: 10 Zeichen
- Komplexität: min 3 Charakteristika aus Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen.
- Passwortsperrung nach 10 Fehlversuchen
- Täglicher Abgleich aller Passwörter gegen Kompromittierungsdatenbanken

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland

1.2.2. Firewall und Netzwerksegmentierung

Der äußere Perimeter des Netzwerks wird durch eine hochverfügbare Firewall gesichert.

Das interne Netzwerk (LAN) ist in mehrere funktionalen Bereiche segmentiert, die eine Trennung nach Funktionen, Kunden und Gästen vorsieht.

1.2.3. Verschlüsselung

Alle Arbeitsplätze werden mit aktivierter Festplattenverschlüsselung ausgegeben. Encryption Keys werden zentral in der IT-Abteilung verwaltet.

Sensible persönliche Arbeitnehmer- und Gesundheitsdaten werden explizit zusätzlich durch das Verschlüsselungsprogramm „Boxcryptor“ verschlüsselt. Encryption Keys sind ausschließlich den Mitarbeitern der Personalabteilung und dem Management zugänglich.

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.3.1. Rollen und Berechtigungskonzept

Zugriffsrechte auf persönliche Daten werden nach Geschäftsfunktionen unterteilt und vergeben. Insbesondere der Zugriff auf Arbeitnehmerdaten ist ausschließlich der Personalabteilung möglich.

1.3.2. Regelmäßige Kontrollen der Berechtigungen

Die Rollenzuordnung von Benutzern wird regelmäßig, quartalsweise auditiert.

Zugriffe für ausgeschiedene Mitarbeiter werden automatisiert umgehend nach Beendigung des Arbeitsverhältnisses deaktiviert.

1.3.3. Aktenvernichtung

Zur Vernichtung von Papierakten steht eine verschlossene Aktenvernichtungstonne zur Verfügung, die protokolliert von einem Aktenvernichtungsdienstleister entsorgt und vernichtet wird.

1.4. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland

1.4.1. VPN

Externer Zugriff auf das Netzwerk erfolgt mittels SSL verschlüsselter VPN-Protokolle und ist an die o.g. Maßnahmen zur Zugangskontrolle gekoppelt sowie zusätzlich durch eine 2-Faktor-Authentifizierung abgesichert.

1.4.2. E-Mail und Dateitransferverschlüsselung

Der Transfer von Dateien zu Drittparteien erfolgt ausschließlich mittels verschlüsselter Protokolle wie HTTPS oder SSL/TLS.

Die E-Mail-Systeme unterstützen opportunistisches TLS, welches automatisch mit der Gegenstelle eine TLS Verschlüsselung vereinbart.

1.4.3. Datenträger

Sicherstellung der ordnungsgemäßen Vernichtung physischer Datenträger durch zertifizierte Entsorgungsunternehmen bzw. Aktenvernichter.

1.5. Trennungskontrolle

Maßnahmen, damit zu unterschiedlichen Zwecken – insbesondere für unterschiedliche Kunden – erhobene bzw. zu verarbeitende Daten getrennt voneinander verarbeitet werden.

1.5.1. Trennung von Produktions- und Testumgebungen

Umgebungen, die persönliche Daten im Auftrag von Kunden verarbeiten, sind unterteilt in Test und Produktionsumgebungen. Auf Testumgebungen werden keine persönlichen Daten verarbeitet.

1.5.2. Mandantentrennung

Persönliche Daten, die im Auftrag für Kunden verarbeitet werden, werden für jeden Kunden auf logisch getrennten Systemen verarbeitet.

Kundensysteme werden grundsätzlich projektspezifisch angelegt, soweit dies nicht individuell für ein Projekt anders geregelt ist.

2. Gewährleistung der Integrität der Systeme und Dienste

Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können.

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland

2.1. Eingabekontrolle

Zugriffe, Änderungen und Löschungen, insbesondere auf Systeme, die Arbeitnehmerdaten führen, werden protokolliert und unterliegen einer Versionskontrolle.

3. Gewährleistung der Verfügbarkeit der Systeme und Dienste

Maßnahmen, die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.

3.1. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

3.1.1. Datensicherung

Die Datensicherung erfolgt rollierend monatlich, wöchentlich und täglich auf Datensicherungsbändern. Monatsbänder werden in einem separaten Brandschutzbereich in einem abgesetzten Stockwerk des Gebäudes gelagert.

3.1.2. USV

Alle relevanten DV-Systeme sind an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen, die einen autonomen Betrieb bei Stromausfall gewährleistet. Bei einem eintretenden Stromausfall werden die DV-Systeme kontrolliert heruntergefahren.

3.1.3. Virenschutz

Alle Arbeitsplätze und DV-Systeme sind mit Antivirusprogrammen versehen, deren Virensignaturen mehrmals täglich aktualisiert werden.

3.1.4. Brandschutz

Einteilung der Betriebsflächen des Rechenzentrums in Brandabschnitte und unter Einsatz von Brandfrüherkennungsanlagen, Brandmeldeanlagen in Rechenzentrum und Büroräumen. Brandlöschsystem im Rechenzentrum und Feuerlöscher in Büroräumen.

4. Auftragskontrolle

Maßnahmen, damit personenbezogene Daten, die im Auftrag verarbeitet werden, nur nach Weisung verarbeitet werden.

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland

4.1. Verarbeitung durch Auftragsverarbeiter

Weitergabe von persönlichen Daten an Auftragsnehmer erfolgt ausschließlich nach Abschluss eines Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO und erfolgten Garantien zur sicheren Datenverarbeitung.

Die Auftragsverarbeitungsverträge werden zentral vorgehalten.

4.2. Verarbeitung als Auftragsverarbeiter

Der Verarbeitung von persönlichen Daten im Auftrag erfolgt ausschließlich nach Abschluss eines Vertrages zur Auftragsverarbeitung mit dem Auftraggeber.

5. Gewährleistung der Belastbarkeit der Systeme und Dienste

Maßnahmen, die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben.

5.1. Angriffsabwehr

Gezielte und automatisierte (DDos) Attacken werden automatisiert durch die Perimeter-Firewall erkannt und unterbunden.

5.2. Proaktive Überwachung

Vitalitätsdaten aller Systeme werden auf zentralen Dashboards visualisiert und automatisch an Administratoren gemeldet, um der Überschreitung von definierten Schwellenwerten entgegenzuwirken und zu vermeiden.

6. Verfahren zur raschen Wiederherstellung der Verfügbarkeit nach einem Zwischenfall

6.1. Automatisiertes Konfigurationsmanagement

Die Konfiguration aller DV-Systeme liegt in versionierten und gesicherten Konfigurationsdateien vor, die es ermöglichen DV-Systeme nach Ausfall oder Verlust automatisiert erneut zu provisionieren.

Persistenzdaten liegen in den o.g. Backup-Maßnahmen vor und können erneut eingespielt werden.

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

7.1. Datenschutzmanagement

Es sind Datenschutzkoordinatoren und betriebliche Datenschutzbeauftragte bestellt, die Mitarbeiter in Datenschutzs Schulungen unterweisen.

Von allen Mitarbeitern wird bei Einstellung eine schriftliche Verpflichtung auf das Datengeheimnis verlangt.

7.2. Interne Revision

Im Zuge der Internen Audits zu ISO27001 und PCI-DSS werden relevante Maßnahmen wie z.B. das Rollen- und Berechtigungskonzept quartalsweise überprüft.

7.3. Externe Prüfungen

Weitere Maßnahmen, insbesondere zur Datensicherung, Arbeitnehmer und Finanzdaten werden jährlich durch eine externe Wirtschaftsprüfungsgesellschaft nach IDW Standard EPS 300 und ISO27001 geprüft.

Kontakt

Telefon +49 611 945 735 - 0

Fax +49 611 945 735 - 10

Mail info@bare.id

Web www.bare.id

Geschäftssitz

Bare.ID GmbH

Kirchgasse 6

65185 Wiesbaden

Deutschland

Impressum

Geschäftsführer Kian T. Gould (CEO)

Registergericht Wiesbaden B HRB 33190

Bank Wiesbadener Volksbank eG

Schillerplatz 4 | 65185 Wiesbaden

IBAN DE15 5109 0000 0005 2908 05

BIC/SWIFT WIBADE5W

Land Deutschland