Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO

Umsetzung der technischen und organisatorischen Maßnahmen bei badenIT als Anlage zum Rahmenvertrag

Für den Rechenzentrumsbetrieb und alle IT- oder Telekommunikationsdienste, die badenIT im Auftrag ausführt, sind IT Service Management-Verfahren (ITSM) und Informationssicherheitsverfahren (IS) nach der Norm ISO/IEC 20000 und ISO/IEC 27001 eingerichtet. Die ITSM- und IS-Instanzen und -Prozesse, wie Security Management oder Service Continuity & Availability Management, unterliegen jährlichen Audits (intern und extern).

Für den Betrieb in den eigenen Einrichtungen (Rechenzentren) und für den Zugang bzw. Zugriff auf die (Kunden-) Systeme gelten folgende organisatorische und technische Maßnahmen als Standard. In einzelnen Serviceverträgen können weitere Maßnahmen nach dem Stand der Technik vereinbart werden.

1. Pseudonymisierung und Verschlüsselung pers. Daten (Art. 32 Abs. 1 lit. a DS-GVO)

- **Pseudonymisierung**

  Die Verarbeitung von Kundendaten im Rahmen der Auftragsverarbeitung erfolgt nach den jeweiligen Vorgaben des Auftraggebers.

- **Verschlüsselung**

  Es kommen symmetrische und asymmetrische Verschlüsselungstechniken zum Einsatz (VPN (AES256)).

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**

  Der Zugang zu den Rechenzentren (RZ) der badenIT wird mittels Zutrittskontrollsystemen (elektronisch codiertem Schlüssel oder Code-Karte mit Ausweisleser) gesteuert: Kontrollierte Schlüsselvergabe und Berechtigungsvergabe per Code-Karte an einen eng begrenzten Personenkreis. In beiden Fällen erfolgt eine Protokollierung des Zugangs. Einrichtungen der Objektsicherung: Vorfeldsicherung durch abgesperrtes Betriebsgelände und Zugang über Pförtnerdienst, Einbruchmeldeanlagen und Einsatz des Sicherheitsdienstes, Videoüberwachung des Eingangsbereiches zum RZ.

- **Zugangskontrolle zu den Anlagen**

  Der Zugang zu den Systemen ist reglementiert und begrenzt auf Administratoren. Berechtigungen werden beschränkt auf die Tätigkeit im Rahmen ihres Administrationsauftrages vergeben. Die Identifikation und Authentifizierung erfolgt über Kennwortzugänge und eindeutige User-IDs. Die Kennwortverfahren sind reglementiert (Sonderzeichen, Mindestlänge, Gültigkeitsdauer).

badenIT GmbH | Tullastraße 61 | D-79108 Freiburg | Tel: +49 (0)761 5035-0 | Geschäftsführer: Peter Lais
HRB Nr. 5535 | Ust-ID 812388035 | Sparkasse Freiburg Nördl. Breisgau | BLZ 68050101 | Kto: 2328364
IBAN: DE20680501010002328364 | SWIFT-BIC: FRSPDE66XXX

- **Zugriffskontrolle**

  Werden im Einzelfall eines Auftrages Daten einer DV-Anlage durch Mitarbeiter der badenIT bearbeitet - im Sinne der Benutzung des Datenverarbeitungsverfahren - erfolgt die Benutzerverwaltung, Identifikation und Authentifizierung grundsätzlich nach den gleichen Prinzipien wie unter „Zugangskontrolle zu den Anlagen“, mit der notwendigen Eingrenzung der Zugriffsberechtigung nach Vorgaben des Auftraggebers (bedarfsgerechte Rechtevergabe). In Abhängigkeit des Datenverarbeitungsverfahrens erfolgt die Vergabe differenzierter Berechtigungen über Benutzerprofile und/oder Rollen. Sofern nicht anders vereinbart, übernimmt badenIT bei Online-Zugriffen des Auftraggebers die Verantwortung für Ausgabe und Verwaltung von Zugriffssicherungscodes und Verschlüsselungsmechanismen.

- **Trennungskontrolle**

  Der Auftraggeber verarbeitet nur Daten innerhalb ihrer Zweckbestimmung. In Abhängigkeit der Systemumgebung werden dedizierte Systeme eingesetzt oder Einrichtungen der internen Mandantenfähigkeit genutzt. Die Systemgestaltung wird so realisiert, dass Daten für unterschiedliche Zwecke getrennt verarbeitet werden. In der Anwendungsentwicklung erfolgt dazu die Funktionstrennung von Produktions- und Testumgebungen.

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**

  Ein physischer Transport der Daten erfolgt nur zum Auftraggeber selbst, wenn dies im Auftrag vorgesehen ist. Der Transport wird nur durch Mitarbeiter der badenIT ausgeführt - mit Übergabe direkt an die vereinbarte Dienststelle des Auftraggebers. Elektronische, automatisierte Übertragung von Daten erfolgt verschlüsselt (z. B. Protokoll SFTP) in einer geschlossenen Prozesskette. Elektronische, manuelle Datenübertragung erfolgt ebenfalls verschlüsselt (HTTPS) nach Identifikation und Authentifizierung des Benutzers. Verbindungen über das Internet werden nur über gesicherte VPN-Tunnel zugelassen. Die Entsorgung von Datenträgern, Backup-Medien und schriftlichen Dokumenten erfolgt über definierte Entsorgungsprozesse. Einrichtungen zum rechtsgültigen signieren elektronischer Dokumente nach dem Signaturgesetz und der Signaturverordnung in Verbindung mit Trustcenter-Dienstleistungen stehen bei Bedarf zur Verfügung.

- **Eingabekontrolle**

  Sofern der Auftrag die Pflege und Verwaltung von Benutzerdaten, Benutzerkonten und/oder Benutzerberechtigungen enthält, werden Änderungen dokumentiert. Darüber hinausgehende Datenverwaltung oder Datenpflege innerhalb eines Datenverarbeitungsverfahrens findet nicht statt, sofern es der jeweilige Vertrag nicht explizit vorsieht und die Vorgaben definiert.

badenIT GmbH | Tullastraße 61 | D-79108 Freiburg | Tel: +49 (0)761 5035-0 | Geschäftsführer: Peter Lais
HRB Nr. 5535 | Ust-ID 812388035 | Sparkasse Freiburg Nördl. Breisgau | BLZ 68050101 | Kto: 2328364
IBAN: DE20680501010002328364 | SWIFT-BIC: FRSPDE66XXX

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

  Technische Einrichtungen im RZ:

  Die Rechenzentren der badenIT sind mit einer Brandfrüherkennungsanlage und einer Brandmeldeanlage ausgestattet und es besteht eine direkte Meldekette bis zur Freiburger Feuerwehr. Löschanlage, Temperaturüberwachung, redundante USV-Anlagen, Notstromgenerator, Klimatisierung und Wassereinbruchsschutz sind nach dem Stand der Technik eingerichtet. Zentrale Komponenten und Knoten sind in die Monitoring-Systeme einbezogen.

  Sichere Systemumgebung:

  Wir setzen ausschließlich Systeme von namhaften und am Markt etablierten Herstellern ein. Die Systeme sind in ihrer Grundkonfiguration schon redundant ausgelegt. Grundsätzlich werden für die Systeme Wartungsverträge abgeschlossen.

  Security Management:

  Nach den Normvorgaben der ISO/IEC 20000 und ISO/IEC 27001 ist das Security Management installiert. Mehrstufige zentrale Firewall-Systeme verschiedener Hersteller sind in Betrieb. Alle Kundennetze sind separat gesichert, Zugriffe erfolgen über Systeme in der DMZ des Kunden. Ein mehrstufiges Virenschutzkonzept (mindestens zwei Scan-Instanzen) sichert die Systeme.

  Capacity Management und Service Continuity & Availability Management:

  Die Umsetzung ist ebenfalls nach der Norm ISO/IEC 20000 und ISO/IEC 27001 realisiert. Für die schnelle Wiederherstellung von Systemen stehen Wiederanlaufpläne und Disaster Recovery Sicherungen (VM-Ware Umgebung) zur Verfügung. Die Kapazitäten auf den Kundensystemen können überwacht werden (Monitoring). Datensicherungsverfahren werden nach Anforderungen in den vereinbarten SLAs eingerichtet. Zu sichernde Systeme und Backup-Systeme/Medien befinden sich grundsätzlich in getrennten Brandabschnitten bzw. auch in getrennten RZ-Lokationen. Duplizierung der Bänder und zusätzliche Auslagerung in einen externen Tresor nach Servicevereinbarung.

5. Wiederherstellung der Verfügbarkeit und dem Zugang zu pers. Daten bei einem technischen Zwischenfall (Art. 32 Abs 1 lit. c DS-GVO)

Unsere zentrale mandantenfähige Infrastruktur ist durch Redundanzmechanismen grundsätzlich hochverfügbar. Der zentrale Zugriff auf die Systeme erfolgt ebenfalls über redundante Zugangssysteme. Für die schnelle Wiederherstellung stehen zusätzlich Disaster Recovery Sicherungen zur Verfügung. Kundensysteme werden individuell nach SLA-Vereinbarungen betrieben.

badenIT GmbH | Tullastraße 61 | D-79108 Freiburg | Tel: +49 (0)761 5035-0 | Geschäftsführer: Peter Lais
HRB Nr. 5535 | Ust-ID 812388035 | Sparkasse Freiburg Nördl. Breisgau | BLZ 68050101 | Kto: 2328364
IBAN: DE20680501010002328364 | SWIFT-BIC: FRSPDE66XXX

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- **ISO-Prozesse**

  Die Betriebsprozesse laufen nach ISO20000 ab und unterliegen dem jährlichen Audit und KVP-Zyklus.

  Die sicherheitsrelevanten Prozesse sind Teil der ISO27001-Vorgaben und werden durch diese jährlich geprüft und sichergestellt.

- **Datenschutz-Management**

  Es existiert eine Konzernrichtlinie für Datenschutz und Informationssicherheit. Für die Einhaltung der gesetzlichen Anforderungen wurde ein Datenschutzbeauftragter benannt. Er sorgt für die entsprechende Dokumentation und Überwachung der Datenschutzanforderungen. Alle Mitarbeiter werden regelmäßig in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Datengeheimnis geschult. Alle Mitarbeiter sind auf Vertraulichkeit, Datengeheimnis sowie Fernmeldegeheimnis und Steuergeheimnis verpflichtet. Eine Datenschutz-Folgeabschätzung wird bei Bedarf durchgeführt.

- **Incident Response Management**

  Das Vorgehen bei Datenschutzvorfällen ist in unseren internen Prozessbeschreibungen beschrieben. Ein Datenschutzvorfall ist eine Situation, die eine ungewollte Veröffentlichung, Verfälschung oder Löschung von personenbezogenen Daten nach der Datenschutz-Grundverordnung (DS-GVO), dem Sozialgeheimnis oder anderen rechtlich relevanten Daten nach sich ziehen kann. In solchen Fällen ist der zuständige Datenschutzbeauftragte für die Bewertung zu informieren und entsprechende Maßnahmen einzuleiten.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

  Datenschutzfreundliche Voreinstellungen werden physikalisch durch den Schutz des Rechenzentrums, die mandantenfähigen Systeme und der detaillierten Berechtigungen innerhalb der Systeme gewährleistet. Das Rollen- und Rechtekonzept schränkt zusätzlich die Zahl der natürlichen Personen mit administrativer Berechtigung ein. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

- **Auftragskontrolle**

  Gemäß der vertraglichen Vereinbarungen wird der Auftragnehmer unter Berücksichtigung von Datenschutz und Datensicherheit ausgewählt und verpflichtet.

7. Datenweitergabe in ein Drittland

Eine Datenweitergabe in ein Drittland erfolgt nicht. Abweichungen zur Datenweitergabe bei den einzelnen Dienstleistungen werden im Verzeichnis von Verarbeitungstätigkeiten des Auftraggebers beschrieben.

badenIT GmbH | Tullastraße 61 | D-79108 Freiburg | Tel: +49 (0)761 5035-0 | Geschäftsführer: Peter Lais
HRB Nr. 5535 | Ust-ID 812388035 | Sparkasse Freiburg Nördl. Breisgau | BLZ 68050101 | Kto: 2328364
IBAN: DE20680501010002328364 | SWIFT-BIC: FRSPDE66XXX

8. Kategorien der Dienstleistungen

Die technischen und organisatorischen Maßnahmen sind für alle Kategorien der Dienstleistungen gültig. Abweichungen der Dienstleistungen und Anpassungen des Sicherheitskonzepts werden im Verzeichnis von Verarbeitungstätigkeiten des Auftraggebers beschrieben.

9. Anpassungen

badenIT behält sich das Recht vor, den Inhalt dieses Dokuments anzupassen, wenn dies - insbesondere in folgenden Fällen - erforderlich ist:

- Änderung der gesetzlichen Grundlagen im Datenschutzrecht
- Änderung der datenschutzrechtlichen Rechtsprechung
- Änderung einer Anforderung einer datenschutzrechtlichen Zertifizierung
- Änderung der technischen und organisatorischen Maßnahmen (TOM)

Soweit badenIT eine Anpassung dieses Dokuments vornehmen möchte, übermittelt badenIT das Anpassungsangebot spätestens 30 Tage vor dem geplanten Inkrafttreten der Anpassung. Die Zustimmung zur Anpassung durch den Auftraggeber gilt als erteilt, wenn dieser nicht vor dem geplanten Zeitpunkt des Inkrafttretens in Textform widerspricht. Hierauf wird die badenIT in dem Anpassungsangebot hinweisen.

badenIT GmbH | Tullastraße 61 | D-79108 Freiburg | Tel: +49 (0)761 5035-0 | Geschäftsführer: Peter Lais
HRB Nr. 5535 | Ust-ID 812388035 | Sparkasse Freiburg Nördl. Breisgau | BLZ 68050101 | Kto: 2328364
IBAN: DE20680501010002328364 | SWIFT-BIC: FRSPDE66XXX