## Implementation of the technical and organizational measures at badenIT as an appendix to the Outline Agreement

For data center operation and all IT or telecommunication services performed by badenIT on commission, IT service management (ITSM) processes und information security (IS) processes as per the standards ISO/IEC 20000 and ISO/IEC 27001 are in place. ITSM and IS instances and processes such as security management and service continuity & availability management are subject to annual audits (internal and external).

The following organizational and technical measures apply by default for operation in the company's own facilities (data centers) and for access to (customer) systems. Further measures concerning the level of technology can be agreed upon in individual service agreements.

### 1. Pseudonymization and encryption of personal data (Art. 32 Section 1 lit. a GDPR)

» **Pseudonymization**

The processing of customer data within the scope of order processing is carried out in accordance with the corresponding provisions of the ordering party.

» **Encryption**

Symmetrical and asymmetrical encryption techniques are used (VPN (AES256)).

### 2. Confidentiality (Art. 32 Section 1 lit. b GDPR)

» **Physical access control**

Physical access to the data centers (DCs) of badenIT is controlled by means of physical access control systems (electronically coded key or code card with ID reader): Controlled key assignment and authorization assignment via code card to an extremely limited circle of persons. In both cases, there is documentation of the physical access. Systems for securing the premises: Front-end security via locked company premises and access via a gate service, intrusion detection systems and the use of a security service, video surveillance at the entrance area to the DC.

» **Control of virtual access to the systems**

Virtual access to the systems is regulated and limited to administrators. Authorizations are granted with restriction to the tasks that fall within the scope of their administrative role. Identification and authentication are via password-protected access and unique user IDs.



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

The password procedures are regulated (special characters, minimum length, validity period).

» **Virtual access control**

If in the individual case of a commission, the data of a DP system is processed by badenIT staff – in the context of using the data processing process – user administration, identification and authentication are generally according to the same principles as under "Control of virtual access to the systems", with the necessary limitation of access authorization as per the specifications of the ordering party (requirements-based assignment of rights). Depending on the data processing process, the assignment of differentiated authorizations is via user profiles and/or roles. Unless otherwise agreed upon, in the case of online access by the ordering party, badenIT is responsible for issuing and managing access security codes and encryption mechanisms.

» **Separation control**

The ordering party processes data only for its intended purpose. Depending on the system environment, dedicated systems or facilities for internal client capability are used. The system design is implemented so that data for different purposes is processed separately. In application development, there is function-based separation of production and test environments.

## 3. Integrity (Art. 32 Section 1 lit. b GDPR)

» **Forwarding control**

Data is physically transported only to the ordering party itself if this is planned for in the order. The transport is carried out by badenIT personnel only – with the handover directly at the agreed upon office of the ordering party. Electronic, automated data transmission takes place under encryption (e.g., SFTP) in a closed process chain. Electronic, manual data transmission also takes place under encryption (HTTPS) following identification and authentication of the user. Connections via the Internet are only permissible via secured VPN tunnels. The disposal of data storage media, backup media and written documents is carried out as per defined disposal processes. Systems for the legally valid signing of electronic documents as per the German Digital Signature Act and Digital Signature Directive in connection with trust center services are available if required.



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

» **Input control**

If the order includes the maintenance and administration of user data, user accounts and/or user authorizations, changes are documented. Data administration beyond this scope or data maintenance within a data processing process does not take place unless the corresponding order plans for it explicitly and defines the specifications.

## 4. Availability and resilience (Art. 32 Section 1 lit. b GDPR)

» **Availability control**

**Technical systems in the DC:**

The data centers of badenIT are equipped with a system for the early detection of fire and a fire alarm system, and there is a direct notification chain which leads to the Freiburg fire department. Extinguishing system, temperature monitoring, redundant UPS systems, emergency power generator, air-conditioning and protection against water ingress are set up according to the best available technology. The main components and nodes are integrated in the monitoring systems.

**Secure system environment:**

We use only systems from reputable manufacturers that are well established on the market. The systems are already designed redundantly in their basic configuration. Maintenance agreements are generally concluded for the systems.

**Security management:**

Security management is installed according to the provisions of the standards ISO/IEC 20000 and ISO/IEC 27001. Centralized multilayer firewall systems from various makers are in operation. All customer networks are secured separately; access is via systems in the customer's DMZ. A multilayer virus protection concept (at least two scan instances) secures the system.

**Capacity management and service continuity & availability management:**

The implementation is likewise executed as per the standards ISO/IEC 20000 and ISO/IEC 27001. Restart plans and disaster recovery backups (VMware environment) are available for fast system restoration. Capacities in customer systems can be monitored. Data backup processes are set up according to the requirements in the agreed upon SLAs. Systems to be backed up and backup systems/media are generally kept in separate in fire sections
and/or also in separate DC locations. Duplication of the tapes and additional storage in an external safe as per service agreement.



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

## 5. Restoration of availability and access to personal data in the case of a technical incident (Art. 32 Section 1 lit. c GDPR)

As a rule, our centralized, client-enabled infrastructure is highly available as a result of redundancy mechanisms. Likewise, centralized access to the systems is via redundant access systems. Disaster recovery backups are additionally available for fast restoration. Customer systems are individually operated in accordance with SLAs.

## 6. Processes for regular testing, assessment and evaluation (Art. 32 Section 1 lit. d GDPR; Art. 25 Section 1 GDPR)

» **ISO processes**

The operating processes run according to ISO20000 and are subject to the annual audit and CIP cycle. The security-relevant processes are part of the ISO27001 specifications and are audited annually and ensured as a result.

» **Data protection management**

There is a group guideline for data protection and information security. For adherence to the applicable requirements, a data protection officer has been named. He is responsible for the corresponding documentation and for monitoring data protection requirements. All staff receive regular training in connection with confidentiality, availability, integrity and data privacy. All staff are required to observe confidentiality, data privacy, the privacy of telecommunications and fiscal privacy. A data protection impact assessment is carried out as required.

» **Incident response management**

How to proceed in case of data protection incidents is described in our internal process descriptions. A data protection incident is a situation which may result in undesired publication, falsification or deletion of personal data as per the General Data Protection Regulation (GDPR), social privacy or other legally relevant data. In such cases, the data protection officer responsible for assessment is to be notified and the corresponding measures are to be initiated.

» **Data-protection-friendly default settings (Art. 25 Section 2 GDPR)**

Data-protection-friendly default settings are ensured physically as a result of data center protection, client-enabled systems and detailed authorizations within the systems. The roles and rights concept additionally restricts the number of natural persons with administrative authorization.
Only as much personal data as is necessary for the respective purpose is collected.



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

» **Order control**

As per contractual agreements, the contractor is selected and committed to compliance regarding data protection and data security.

## 7. Forwarding of data to a third country

Data is not forwarded to any third country. Deviations to the forwarding of data in the case of individual services are described in the directory of the processing tasks of the ordering party.

## 8. Service categories

The technical and organizational measures are valid for all categories of services. Deviations concerning services and adaptations to the security concept are described in the directory of processing tasks of the ordering party.

## 9. Adaptations

badenIT reserves the right to adapt the content of this document if this is necessary – especially in the following cases:

- Change in data privacy legislation
- Change in data privacy case law
- Change in a requirement for applicable data privacy certification
- Change in technical and organizational measures (TOMs)

In the event that badenIT intends to adapt this document, badenIT will send the adaptation proposal no later than 30 days before the adaptation goes into effect. The ordering party's consent to the adaptation is deemed granted unless the ordering party submits an objection in writing before the point in time when the adaptation is scheduled to go into effect. badenIT will indicate this in the adaptation proposal.



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