Technische und organisatorische Maßnahmen zum Schutz der Daten

Die lohn-ag.de AG, Flugstraße 15, 76532 Baden-Baden, ist verpflichtet, für ihren Verantwortungsbereich die nach der Datenschutzgrundverordnung erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Diese sind nachfolgend beschrieben.

Bearbeitungsstand: 28.03.2018

1. Vertraulichkeit (Art. 32. Abs, 1 lit. B DSGVO)

- **Zutrittskontrolle**
  Der Zutritt zu den Geschäftsräumen der lohn-ag ist ausschließlich für berechtigte Personen möglich und durch eine protokollierte Kontrolle gesichert. Zutritt zu den Datenverarbeitungsanlagen ist ausschließlich für gesondert berechtigte Personen möglich und durch eine protokollierte Kontrolle gesichert (PIN oder Schlüssel).

- **Zugangskontrolle**
  Der Zugang zu den Systemen erfolgt mittels sicherer Passwort-Authentifizierung. Bei einem elektronischen Datenaustausch zwischen dem lohn-ag Rechenzentrum und dem Kunden besteht das Sicherungssystem aus unterschiedlichen, mehrschichtigen und komplexen Prüfungen. Weitere technische Absicherungen erfolgen über Firewalls und Proxyserver. Soweit dies technisch möglich und wirtschaftlich vertretbar ist, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt

- **Zugriffskontrolle**
  Das Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems erfolgt nur durch befugte Personen. Die Zugriffskontrolle erfolgt durch Berechtigungskonzepte bedarfsgerechte Zugriffsrechte und die Protokollierung von Zugriffen / Benutzeranmeldungen am System. Personenbezogene Daten befinden sich nur am Arbeitsplatz des zuständigen Sachbearbeiters und auf den Servern.

- **Trennungskontrolle**
  Die Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten erfolgen getrennt. Die Kunden sind durch physikalisch getrennte Server, virtuelle Server/Sandboxing, Zugriffsberechtigungen, Netzwerktrennungen getrennt.

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**
  Als Auftragsverarbeiter trifft die lohn-ag zusätzlich zu Maßnahmen, die sich aus den jeweiligen Leistungsverzeichnissen der Software / Service ergeben oder durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine Maßnahmen zur Pseudonymisierung.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**
  Ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport findet nicht statt. Der Fernzugriff auf das EDV-System der lohn-ag erfolgt verschlüsselt über Virtual Private Networks (VPN).

- **Eingabekontrolle**
  Die Kontrolle ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, erfolgt Anhand des protokollierten Zugangs des Nutzers. Es wird festgehalten, unter welcher Benutzerkennung wann welche Daten eingegeben, geändert oder entfernt wurden.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**
  Die Daten sind gegen zufällige oder mutwillige Zerstörung durch Sabotage bzw. sonstigen Verlust geschützt durch online/offline und on-site/off-site Backup-Strategien, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne, Brand- und Wasserschutz, Einbruchmeldesysteme.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**
  Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden.

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle: Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers