Allgemeine Beschreibung
der technischen und organisatorischen Maßnahmen
gemäß Art. 32 (1) DS-GVO für Auftragsverarbeiter (Art. 30 (2) lit. DS-GVO)

DSB Münster GmbH

Martin-Luther-King-Weg 42/44

48155 Münster

Version 1.1, Stand Juni 2018

Gültig ab 01.06.2018

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält DSB MÜNSTER sich vor, sofern das Schutzniveau nach DS-GVO nicht unterschritten wird.

1. Pseudonymisierung

Als Auftragsverarbeiter trifft DSB MÜNSTER zusätzlich Maßnahmen, die sich aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen ergeben oder durch den Verantwortlichen im Rahmen der Beauftragung zur Pseudonymisierung vorgegeben werden.

2. Verschlüsselung

Regelungsgegenstand:
Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:
Hierzu setzt DSB MÜNSTER für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutzniveau erreichen, das den Anforderungen von Angehörigen an den Schutz von Berufsgeheimnissen angemessen ist.

Dies sind für den elektronischen Transport zwischen DSB MÜNSTER und unseren Kunden/ Rechenzentrum

- und Verantwortlichem: über VPN- oder TLS-Verbindung mit Zwei-Faktor-Authentisierung abgesichert.
- und Institutionen im Auftrag des Verantwortlichen: sichere Übertragung nach den Vorgaben und Standards der Institutionen (z. B. Finanzbehörden, Sozialversicherungsträger, …)
- und Einzelpersonen: personenbezogene Daten der Nutzer über Internet, abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
- und Dienstleistern der DSB MÜNSTER: VPN- oder TLS-Verbindung mit Zwei-Faktor-Authentisierung,
- und Mitarbeitern der DSB MÜNSTER: Verschlüsselte Verbindung mit Zwei-Faktor-Authentisierung

Für den Transport per E-Mail werden Daten, die dem Berufsgeheimnis des Verantwortlichen unterliegen, grundsätzlich nach dem Stand der Technik verschlüsselt.

Mobile Endgeräte der DSB MÜNSTER-Mitarbeiter werden verschlüsselt.

Außerhalb des elektronischen Transports werden Verschlüsselungsverfahren eingesetzt, wenn dies in den Leistungsbeschreibungen der vereinbarten Leistungen dokumentiert ist.
Festplatten von Remote-Arbeitsplatz-Rechnern (Laptops) werden standardisiert nur vollverschlüsselt eingesetzt.

3. Vertraulichkeit

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten.

3.1 Physikalische Sicherheit

Regelungsgegenstand:
Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten.

Technische und organisatorische Maßnahmen:

- Bauliche Maßnahmen

Alle im Auftrag verarbeiteten Daten werden grundsätzlich in Sicherheitsbereichen gespeichert. Der Zutritt ist nur Berechtigten möglich und wird visuell überwacht.

- Objektschutz

Es erfolgt eine Überwachung des Objektes durch technische Einrichtungen..

- Zutrittsregelung zu den kontrollierten Bereichen und Sicherheitsbereichen

Die Zutrittskontrollen zu den DSB MÜNSTER-Standorten und zu den Gebäuden sind lückenlos.

- Das Sicherungssystem ist schalenförmig aufgebaut:
  - DSB MÜNSTER-Mitarbeiter arbeiten grundsätzlich in kontrollierten Bereichen.
  - Sofern Mitarbeiter Remote-Arbeitsplätze außerhalb der kontrollierten Bereiche benutzen, sind sie zur Beachtung besonderer Sicherheitsvorschriften verpflichtet. Die Festplatten der Remote-Arbeitsplatz-Rechner sind vollverschlüsselt.
  - Im Auftrag verarbeitete Daten werden grundsätzlich in Sicherheitsbereichen verarbeitet, die innerhalb der kontrollierten Bereiche durch zusätzliche Maßnahmen wie eingeschränkten Zutrittsberechtigungen geschützt werden.

Die Authentisierung für das Betreten und Verlassen von Sicherheitsbereichen erfolgt über ein Schlüsselkonzept, Fremdleister werden in Sicherheitsbereichen grundsätzlich durch DSB MÜNSTER-Mitarbeiter begleitet.

Es existiert ein geregelter Ablauf zur Genehmigung, Verwaltung und Löschung von Zutrittsberechtigungen. Nicht genutzte Zutrittsberechtigungen werden gelöscht. Vorgesetzte müssen periodisch die Notwendigkeit von Zutrittsberechtigungen für die Mitarbeiter prüfen und bestätigen.

Nicht bei DSB MÜNSTER beschäftigte Personen (Fremdleister wie z. B. Techniker, Besucher) unterliegen der Besucherbegleitpflicht bzw. der Aufsichtspflicht durch die beauftragenden Fachabteilungen.

3.2 Authentifizierung

Regelungsgegenstand:
Es muss verhindert werden, dass Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten) von unbefugten Dritten genutzt werden können.

Technische und organisatorische Maßnahmen:

- Technische Maßnahmen (innerhalb von kontrollierten Bereichen)

Alle Rechner verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort). Es gibt vorgeschriebene Regeln zur Passwortvergabe. Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.

Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen Penetrationen durchgeführt.

- Technische Maßnahmen (außerhalb von kontrollierten Bereichen)

Ein Zugang zu Systemen und Diensten, mit denen im Auftrag verarbeitete Daten mit Berufsgeheimnissen verarbeitet werden, wird ausschließlich nach Zwei-Faktor-Authentisierung („Besitz und Wissen“) gestattet.

Für andere Kategorien von im Auftrag verarbeiteten Daten können die Verfahren für die Datenübertragung, die Sicherungsmechanismen und die Zugangskontrollen in den Leistungsbeschreibungen dargestellt werden.

- Organisatorische Maßnahmen

Es sind definierte organisatorische und technische Verfahren und Methoden zum Incident-Management umgesetzt.

Die IT-Systeme werden auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.

DSB MÜNSTER hat mit den Herstellern und Providern grundsätzlich Verträge geschlossen. Hierbei werden DSB MÜNSTER bekannte Schwachstellen gemeldet, um geeignete Maßnahmen zur Risikoreduzierung und Fehlerbehebung zu treffen.

3.3 Berechtigungskonzept

Regelungsgegenstand:
Die zur Benutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen. Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Technische und organisatorische Maßnahmen:

- Technische Maßnahmen

Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, welche es ermöglicht, Datenzugriffe und –veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben. Es gibt vorgeschriebene Regeln zur Passwortvergabe. Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.

- Organisatorische Maßnahmen zur Zugriffsberechtigung

Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Die Erteilung der Berechtigungen erfolgt in einem dokumentierten Genehmigungsverfahren. Das Erfordernis der Berechtigung wird regelmäßig überprüft.

Zugriffe auf im Auftrag verarbeitete Daten, die zur Serviceerbringung und Auskunftserteilung an Verantwortliche erfolgen, werden grundsätzlich protokolliert und ausschließlich zu Zwecken der Datenschutzkontrolle verwendet.

Die persönliche Verantwortung jedes Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird durch Schulungsmaßnahmen, Infomärkte und zentral bereitgestellte Informationen gestärkt.

3.4 Weitergabe von Daten

Regelungsgegenstand:
Im Auftrag verarbeitete Daten dürfen bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische und organisatorische Maßnahmen:

- Datenübertragung

Die Datenübertragung zwischen DSB MÜNSTER und anderen Kommunikationspartnern wird grundsätzlich verschlüsselt (Siehe Abschnitt 2 „Verschlüsselung“). Dabei kann DSB MÜNSTER das konkrete Verfahren mit den Partnern individuell regeln.

Ferner werden die in Ziffer 2 aufgeführten Verschlüsselungsmaßnahmen getroffen.

- Datenträgertransport
- Es bestehen verbindliche Sicherheitsregelungen für den Transport von vertraulichen Datenträgern.
    - Überbekleidung und Gepäckstücke müssen vor Betreten eines Sicherheitsbereiches abgelegt werden.

3.5 Löschen von Daten

Regelungsgegenstand:
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Technische und organisatorische Maßnahmen:
Vernichten von Datenträgern

Datenträger werden zentral in einem eigens hierfür definierten Bereich gelagert. Alle Datenträger werden in Übereinstimmung mit der DIN-Norm SPEC 66399 "Büro- und Datentechnik – Vernichtung von Datenträgern Teil 3: Prozess der Datenträgervernichtung, Februar 2013" nach Schutzklasse 3 und Sicherheitsstufe 4 vernichtet.

3.6 Mandantentrennung

Regelungsgegenstand:
Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Technische und organisatorische Maßnahmen:
Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene Aufgabenerfüllung unbedingt erforderlich ist.

Bei der Nutzung der DSB MÜNSTER-Infrastruktur (Hard-/Software) werden bereits zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Kundennummer) erhobene bzw. gespeicherte Daten logisch getrennt verarbeitet.

4. Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

Hierzu trifft DSB MÜNSTER Maßnahmen für ein Schutzniveau, das jeweils abhängig von dem Risiko für die Rechte und Freiheiten der betroffenen Personen.

4.1 Protokollierung

Regelungsgegenstand:
Es sind Maßnahmen zu wählen, mittels derer nachträglich überprüft und festgestellt werden kann, ob und von wem im Auftrag verarbeitete Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische und organisatorische Maßnahmen:
Bei den IT-Systemen erfolgt eine laufende Protokollierung der Abläufe.

Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

5. Verfügbarkeit

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

Hierzu trifft DSB MÜNSTER Maßnahmen, die dazu dienen, dass im Auftrag verarbeitete Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn der Verantwortliche sie benötigt.

5.1 Sicherstellen der Verfügbarkeit

Regelungsgegenstand:
Im Auftrag verarbeitete Daten sind gegen zufällige oder mutwillig herbeigeführte Zerstörung oder Verlust zu schützen.

Technische und organisatorische Maßnahmen:

- Geografische Maßnahmen

Die Systeme und Daten der DSB MÜNSTER werden an geografisch getrennten Orten verarbeitet und gesichert.

- Personelle Maßnahmen

Durch regelmäßige Wartung der Systeme besitzen die technischen Anlagen der DSB MÜNSTER eine hohe Verfügbarkeit. Dies wird durch DSB MÜNSTER-eigene Techniker und entsprechende Serviceverträge für Wartung und Entstörung mit den Providern sichergestellt.

Die Abwicklung der Aufträge wird überwacht und begleitet, die korrekte Umsetzung der vertraglich vereinbarten Leistungen wird kontrolliert. Abweichungen werden zeitnah geklärt.

- Organisatorische Maßnahmen

Die Maßnahmen für den Fall physischer oder technischer Zwischenfälle werden in geregelten Abständen überprüft.

Sind spezielle organisatorische Maßnahmen zur Erfüllung der vertraglich vereinbarten Leistung notwendig, so werden diese individuell mit dem Auftraggeber festgelegt.

- Notstrom

Die Stromversorgung für die IT-Systeme ist redundant aufgebaut und erlaubt über dynamische USV-Anlagen (Unterbrechungsfreie Stromversorgung) die Leistungsversorgung.

5.2 Zweckbindung

Regelungsgegenstand:
Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies gilt insbesondere auch für die Löschung von Daten.

Technische und organisatorische Maßnahmen:
Die Verarbeitung von Auftragsdaten erfolgt ausschließlich entsprechend den Leistungsvereinbarungen mit dem Auftraggeber.

Weisungen zur Verarbeitung und insbesondere zur Löschung von im Auftrag verarbeiteten Daten werden nur ausgeführt, wenn der Kunde sie in der vertraglich vorgeschriebenen Form erteilt.

Kontrollen:

DSB MÜNSTER räumt im Rahmen der Regelungen der Vereinbarung zur Auftragsdatenverarbeitung der DSB MÜNSTER den autorisierten Ansprechpartnern des Auftraggebers und dem Datenschutzbeauftragten nach vorheriger Anmeldung und Abgabe einer Datenschutzerklärung/ Verschwiegenheitserklärung zu den üblichen Geschäftszeiten auf Verlangen ein Zutrittsrecht sowie ein Auskunfts- und Kontrollrecht ein, um dessen Überwachungspflicht beim Auftragnehmer erfüllen zu können. Der Zutritt zu den Produktionsräumen der DSB MÜNSTER erfolgt nur in Begleitung von DSB MÜNSTER-Personal.

6. Belastbarkeit der Systeme

Regelungsgegenstand:
Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch

Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder –abstürzen ist zu reduzieren.

Hierzu trifft DSB MÜNSTER für die Verarbeitung von Daten im Maßnahmen für eine Systemstabilität, die dem Anspruch zuverlässig zeitgerechte Verarbeitung der Daten gerecht wird.

Technische und organisatorische Maßnahmen:
DSB MÜNSTER führt eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. DSB MÜNSTER hat ein Notfallkonzept umgesetzt, das z. B. Maßnahmen zur Abwehr von Angriffen (z. B. Virenscanner, Firewall) beinhaltet. Dieses Notfallkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Regelungsgegenstand:
Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

Hierzu trifft DSB MÜNSTER für die Verarbeitung von Daten im Auftrag Maßnahmen für die Systemstabilität, die dem Anspruch an zuverlässig zeitgerechte Verarbeitung ihrer Daten gerecht wird.

Technische und organisatorische Maßnahmen:
Die personenbezogenen Daten werden grundsätzlich in geographisch getrennten Standorten gesichert.

Nach einem physischen oder technischen Ausfall eines Teil-Rechenzentrums übernimmt die verbliebene Infrastruktur die Verarbeitung. Für alle IT- und TK-Systeme besteht ein Wiederanlaufkonzept. Das Wiederanlaufkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.

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

Regelungsgegenstand:
Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Technische und organisatorische Maßnahmen:
Die Wirksamkeit der Maßnahmen wird u.a. durch den Datenschutzbeauftragten und durch den Informationssicherheitsbeauftragten der DSB MÜNSTER laufend geprüft.

9. Dokumentation

Es liegen schriftlich vor:

X interne Verhaltensregeln
X Risikoanalyse
X allgemeine Datensicherheitsbeschreibung
X umfassendes Datensicherheitskonzept