Anhang zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Technisch-organisatorische Maßnahmen

Version	Datum	Kommentar
Aktuelle Version (v. 1)	**07.12.02017 11:58**	**Gerhard Schwärzler**: Anhang 1 zum AV-Vertrag vom 07.12.2017

Inhalt

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

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, durch kontrollierte Schlüsselvergabe.

Zugangskontrolle

Keine unbefugte Systembenutzung durch

- Einrichtung eines Benutzerstammsatzes pro User, soweit dies in vertretbarem Aufwand und unter Berücksichtigung der Risiken möglich ist.
- Kennwortverfahren, möglichst über sehr große Kennwortlängen (ganze Sätze)
- Punkt zu Punkt Verschlüsselung mit client-side certificates.

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Maßnahmen zur bedarfsorientierten Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Differenzierte Berechtigungen (DB-, OS-oder Applikations-User)

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten zu unterschiedlichen Zwecken:

- Mandantenfähigkeit auf Ebene DB-Schema und Applikationen
- Funktionstrennung: Produktion, Demo/Test und Entwicklung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die in der Leistungsvereinbarung festgehaltenen Leistungen erfordern häufig einen Personenbezug, sodass ein Pseudonymisierungsverfahren nicht angewendet wird.

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

Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselung, Tunnelverbindung

Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Bei Veränderungen durch die Applikationen: Protokollierung, soweit bereitgestellt
- DB-Änderungen: Protokollierung durch DBMS

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Backup-Verfahren;
- Spiegeln von Festplatten, RAID-Verfahren;
- Unterbrechungsfreie Stromversorgung (USV);
- Firewall

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Maßnahmen: virtualisierter Betrieb mit regelmäßiger Sicherung „kalter“ VM-Images.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Ergebnisse von Überprüfungen (wie zB Penetrationstests) werden in regelmäßigen Abständen bewertet und die notwendigen Anpassungsmaßnahmen werden vorgenommen.

Incident-Response-Management

Vergangene Vorfälle werden im Rahmen regelmäßiger Audits bewertet und die notwendigen Anpassungsmaßnahmen werden vorgenommen.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- Rollen-Rechtekonzept mit Einschränkung des Zugriffs auf personenbezogene Daten abhängig von der Benutzerfunktion (Rolle)
- Funktionen zur Wahrung der Betroffenenrechte auf
    - Auskunft: Personenportraits in den Administrationsapplikationen
    - Löschung: work-around über Dublettenzusammenführung auf eine Pseudoperson
    - Sperrung von Daten durch Anonymisierung in den öffentlichen Ansichten
- Steuerung der Sichtbarkeit personenbezogener Daten im persönlichen Zugang von Systembenutzern.

Auftragskontrolle

Maßnahmen (technisch, organisatorisch) zur Abgrenzung der Kompetenzen zwischen VERBAND und NU:

- Eindeutige Vertragsgestaltung (Wartungs- und Regievertrag)
- Formalisierte Auftragserteilung (JIRA Software, NU Projekte)
- Kontrolle der Vertragsausführung (Abnahme auf Demosystem bei Entwicklungen)