Verwaltungsverordnung über die Auftragsverarbeitung personenbezogener Daten durch das Erzbistum Paderborn im Zusammenhang mit den Wahlen der Kirchenvorstände und der pastoralen Gremien im Erzbistum Paderborn (AV-VO)

Vom 30. Mai 2025

KA 2025, Nr. 79

§ 1
Gegenstand der Regelung und Dauer der Verarbeitung

(1) [1]Im Rahmen der Wahlen der Kirchenvorstände und der pastoralen Gremien gemäß den Bestimmungen der KV-WahlDVO vom 19. März 2025 (KA 2025, Nr. 48) und der PG-WahlDVO vom 19. März 2025 (KA 2025, Nr. 49), geändert am 09. Mai 2025 (KA 2025, Nr. 70), führt das Erzbistum Paderborn als Auftragsverarbeiter für die Kirchen-/Pfarrgemeinden (Verantwortliche gemäß § 4 Ziffer 9 KDG) die in Anlage 1 aufgeführten Datenverarbeitungen durch. [2]Dies umfasst im gegebenen Fall auch die aus den Kirchen-/Pfarrgemeinden erfolgende Bildung von pastoralen Gremien auf Ebene der Pastoralen Räume.

(2) Die Auftragsverarbeitung beginnt nach zustimmender Erklärung des jeweiligen Kirchenvorstandes.

(3) Diese Verordnung ist Rechtsinstrument im Sinne des § 29 Abs. 3 KDG und gesonderte Regelung im Sinne des § 13a Abs. 2 KV-WahlDVO und § 13a Abs. 2 PG-WahlDVO.

§ 2
Weisungen des Verantwortlichen

(1) [1]Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich für die in § 2 aufgeführten Zwecke bzw. nur auf Grund dokumentierter Weisungen der Verantwortlichen, es sei denn, er ist nach dem kirchlichen Recht, dem Recht der Europäischen Union oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. [2]In einem solchen Fall teilt der Auftragsverarbeiter den Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen kirchlichen oder öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert die Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der katholischen Kirche, der Europäischen Union oder eines Mitgliedstaats verstößt.

(3) Die Verantwortlichen informieren den Auftragsverarbeiter unverzüglich, wenn sie Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter feststellen.

(4) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 3
Technisch-organisatorische Maßnahmen

(1) [1]Der Auftragsverarbeiter bietet hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des KDG erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. [2]Hierzu trifft er mindestens die im Anlage 3 aufgeführten technischen und organisatorischen Maßnahmen. [3]Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. [4]Bei der Beurteilung des angemessenen Schutzniveaus ist dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach § 11 KDG i.V.m. § 4 Nr. 2 KDG bzw. § 12 KDG) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen hinreichend Rechnung zu tragen.

(2) [1]Die in Anlage 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. [2]Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. [3]Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. [4]Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 4
Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) [1]Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Auftrags unbedingt erforderlich ist. [2]Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen perso-

nenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) [1]Der Auftragsverarbeiter teilt den Verantwortlichen die Kontaktdaten seines betrieblichen Datenschutzbeauftragten mit. [2]Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über einen etwaigen Wechsel des betrieblichen Datenschutzbeauftragten.

(4) [1]Der Auftragsverarbeiter ist verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten gemäß § 31 Abs. 2 KDG zu führen. [2]Dieses Verzeichnis haben die Verantwortlichen und ihr betrieblicher Datenschutzbeauftragter vorab erhalten. [3]Der Auftragsverarbeiter pflegt das Verzeichnis fortlaufend und stellt den Verantwortlichen und ihrem betrieblichen Datenschutzbeauftragten angepasste Versionen unaufgefordert und der Datenschutzaufsicht auf Anfrage zur Verfügung.

(5) [1]Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. [2]Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung der Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen des KDG erfüllt sind.

§ 5
Unterstützungspflichten des Auftragsverarbeiters

(1) [1]Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter die Verantwortlichen bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Datenschutzaufsicht und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. [2]Der Auftragsverarbeiter unterrichtet die Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit die Verantwortlichen ihre bestehenden Pflichten gegenüber den betroffenen Personen erfüllen können.

§ 6
Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) [1]Der Auftragsverarbeiter darf Unterauftragsverarbeiter, die nicht in der Anlage 2 benannt sind, nur beauftragen, wenn die Verantwortlichen die Beauftragung vorher schriftlich genehmigt haben. [2]Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden, rechtzeitig, mindestens jedoch drei Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters, zur Verfügung. [3]Die Inanspruchnahme der in der Anlage 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieser Verordnung genannten Voraussetzungen umgesetzt werden.

(2) [1]Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in dieser Regelung erfolgten Festlegungen auch gegenüber dem Unterauftragsverarbeiter gelten. [2]Der Auftragsverarbeiter stellt den Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. [3]Der Auftragsverarbeiter haftet gegenüber den Verantwortlichen im Rahmen des § 29 Abs. 5 S. 2 KDG dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. [4]Der Auftragsverarbeiter benachrichtigt die Verantwortlichen über etwaige vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten in einen Drittstaat beinhaltet, die Einhaltung der Regelungen des § 29 Abs. 11 KDG i.V.m. § 40 Abs. 1 KDG sicher.

(4) Der Auftragsverarbeiter schließt in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne des Kapitels 5 des KDG beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach § 40 Abs. 2 lit. a KDG i.V.m. Art. 46 Abs. 2 lit. c DSGVO, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) [1]Im Falle des § 6 Abs. 3 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln der jeweils zuständigen Aufsichtsbehörden durch und stellt diese den Verantwortlichen unaufgefordert zur Verfügung. [2]Kommen Auftragsverarbeiter oder Verantwortliche zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. [3]Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

§ 7
Kontrollrechte der Verantwortlichen

(1) [1]Der Auftragsverarbeiter stellt den Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus dem KDG ergebenden Pflichten erforderlich sind. [2]Auf Verlangen der Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. [3]Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des § 29 Abs. 6 KDG des Auftragsverarbeiters berücksichtigen.

(2) [1]Die Verantwortliche können die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. [2]Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Beteiligten stellen der zuständigen Datenschutzaufsicht die in dieser Regelung genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8
Mitzuteilende Verstöße

(1) [1]Der Auftragsverarbeiter unterrichtet die Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten der Verantwortlichen. [2]Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) [1]Dem Auftragsverarbeiter ist bekannt, dass die Verantwortlichen verpflichtet sind, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. der Datenschutzaufsicht bzw. der betroffenen Person zu melden. [2]Er wird Verletzungen unverzüglich an die Verantwortlichen melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9
Beendigung des Auftrags

(1) [1]Kopien oder Duplikate der Daten werden ohne Wissen der Verantwortlichen nicht erstellt. [2]Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) [1]Mit Beendigung der Auftragsverarbeitung oder früher nach zulässiger Aufforderung durch die Verantwortlichen hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl der Verantwortlichen entweder datenschutzkonform zu löschen oder zurückzugeben, soweit nicht nach dem kirchlichen Recht oder dem Recht der Europäischen Union oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. [2]Dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. [3]Im Hinblick auf die Anbietungspflichten der Verantwortlichen gegenüber dem zuständigen kirchlichen Archiv erfolgt die Löschung durch den Auftragsverarbeiter erst nach entsprechender Freigabe durch die Verantwortlichen. [4]Nach Ablauf einer angemessenen Aufbewahrungsdauer sind die Verantwortlichen zur Rücknahme der Daten verpflichtet. [5]Die Löschung hat der Auftragsverarbeiter den Verantwortlichen in Textform anzuzeigen.

(3) [1]Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. [2]Er kann sie zu seiner Entlastung bei Auftragsende den Verantwortlichen übergeben.

§ 10
Inkrafttreten

Diese Verwaltungsverordnung tritt mit Veröffentlichung im Kirchlichen Amtsblatt in Kraft.

Anlage 1
Auflistung der beauftragten Verarbeitungen

Lfd. Nr.	*Gegenstand/ Art*	*Dauer*	*Zweck*	*Datenkategorien (Art)*	*Kreis der Betroffenen*
1	Hosting und Support	§ 20 Abs. 2 WahlO bis Ablauf der Wahlperiode	Durchführung der Wahlen der Kirchenvorstände und der pastoralen Gremien in den Kirchengemeinden und den pastoralen Räumen des Erzbistums Paderborn mit der Anwendung „ELEKTRA Wahlmanagement“	Name/Vorname, Email-Adresse, zugehörige Kirchengemeinde	Standortverantwortliche
				Name/Vorname, Angabe des Erstwohnsitzes, Einspruchsinhalt	Wahlberechtigte (außer Sperrvermerke nach § 51 BMG)
				Name/Vorname, Beruf, Erstwohnsitz (Ort/Ortsteil), mit Einwilligung zusätzliche Daten wie Foto, Angaben zu Motiven für Kandidatur Erklärung zu Wählbarkeitsvoraussetzungen gemäß § 11 KVVG Erreichte Stimmenzahl, ggf. Einspruchsinhalt bei Einlegung eines Einspruchs	KandidatInnen
				Name/Vorname, Erstwohnsitz	Unterzeichner Vorschlagsliste, Unterzeichner Ergänzungsvorschlag
				Name/Vorname, Adresse, Alter, Vermerk	Wahlberechtigte

Lfd. Nr.	*Gegenstand/ Art*	*Dauer*	*Zweck*	*Datenkategorien (Art)*	*Kreis der Betroffenen*
				Name/Vorname, ggf. Adresse (wenn Zusendung gewünscht)	AntragstellerInnen Briefwahl
				Name, Vorname, Anschrift, Telefonnummer, E-Mailadresse, Beruf und Geburtsdatum	neu gewählte Kirchenvorstands- bzw. Mitglieder pastoraler Gremien und Ersatzmitglieder
2	Druck- und Versanddienstleistungen	§ 20 Abs. 2 WahlO bis Ablauf der Wahlperiode	Zustellung Wahlunterlagen	Name/Vorname, Adresse	Briefwähler
			Zustellung Wahlbenachrichtigung		Wahlberechtigte

Anlage 2
Auflistung der Unterauftragsverarbeitungen

Lfd. Nr.	*Gegenstand /Art*	*Firmierung und Sitz der Unterauftragsverarbeiter*	*Ort der Datenverarbeitung (Land)*	*Gewährleistung eines angemessenen Datenschutzniveaus bei Datenverarbeitung außerhalb der EU/des EWR*
1	Hosting und Support im Rahmen der Online-Wahlen	Electric Paper Informationssysteme GmbH Konrad-Zuse-Allee 15 21337 Lüneburg Deutschland Geschäftsführer: Lars Riemenschneider USt-IdNr.: DE 284198251 HRB-Nr. 203863, Amtsgericht Lüneburg Telefon: +49 4131 96916 0	Deutschland	
2	Hosting	Bistum Essen Zwölfling 16 45127 Essen Tel.: 0201/2204-0 Körperschaft des öffentlichen Rechts, vertreten durch Generalvikar Msgr. Klaus Pfeffer E-Mail: generalvikariat@bistum-essen.de	Deutschland	

Lfd. Nr.	*Gegenstand /Art*	*Firmierung und Sitz der Unterauftragsverarbeiter*	*Ort der Datenverarbeitung (Land)*	*Gewährleistung eines angemessenen Datenschutzniveaus bei Datenverarbeitung außerhalb der EU/des EWR*
3	Druck- und Versanddienstleistungen	Electric Paper Informationssysteme GmbH Konrad-Zuse-Allee 15 21337 Lüneburg Deutschland Geschäftsführer: Lars Riemenschneider USt-IdNr.: DE 284198251 HRB-Nr. 203863, Amtsgericht Lüneburg Telefon: +49 4131 96916 0	Deutschland	

Anlage 3
Allgemeine technische und organisatorische Maßnahmen gemäß § 26 KDG

Geltungsbereich: Bereich IT und Datensicherheit

1. Vertraulichkeit

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ☒ Alarmanlage Video-/Fernsehmonitor mit Aufzeichnung [RZ Bereich]
- ☒ Automatisches Zugangskontrollsystem
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Schließsystem mit Codesperre für Alarmanlage [einzelne RZ Räumlichkeiten]
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge, RZ + Ausweich RZ
- ☒ Lichtschranken / Bewegungsmelder für RZ Räumlichkeiten
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Personenkontrolle beim Einlass / Pförtner / Empfang
- ☒ Zugangskontrolle von Gästen durch Video-Gegensprechanlage + Abholpflicht von Gästen am jeweiligen Eingang

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ☒ Zuordnung von Benutzerrechten
- ☒ Erstellen von Benutzerprofilen
- ☒ Passwortvergabe, Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Authentifikation mit biometrischen Verfahren
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Automatische Sperrung [Bildschirm] (z. B. Kennwort oder Pausenschaltung)
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☒ Verschlüsselung von Smartphone-Inhalten
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einsatz von Anti-Viren-Software
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- ☒ Erstellen eines Berechtigungskonzepts; Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Zugänge nach Funktion mit Passwortvergabe (Tools, Services, ...), Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern [im Bereich IT und Datensicherheit]
- ☒ Löschung von Datenträgern vor Wiederverwendung
- ☒ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Protokollierung der Vernichtung
- ☒ Verschlüsselung von Datenträgern, Verschlüsselung von Datenträgern in Laptops / Notebooks

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

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

- ☒ Logische Mandantentrennung (softwareseitig) für ausgewählte Fachanwendungen
- ☒ Erstellung eines Berechtigungskonzepts für ausgewählte Fachanwendungen und den Verzeichnisdienst
- ☒ Getrennte Netze IT-Management-Netz, Standardnutzer-Netz, separates Gast WLAN, Mobile Endgeräte (Smartphone, Tablets)

2. Integrität

Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...

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

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln (IPSec, SSL)
- ☒ E-Mail-Verschlüsselung, Signatur
- ☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

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

- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts im Verzeichnisdiensts
- ☒ Dokumentenmanagement (eAkte, digitale Personalakte)

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch):

- ☒ Unterbrechungsfreie Stromversorgung (USV) (Netzersatzanlage)
- ☒ Klimaanlage in Serverräumen
- ☒ Redundanter Serverraum mit separatem Kühlsystem für den Notbetrieb
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte / Löschanlage in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Testen von Datenwiederherstellung
- ☒ IT Betriebshandbuch
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen

Wiederherstellung

In Folge eines technischen Defekts oder einer Cyberattacke muss die verantwortliche Stelle in der Lage sein, die Daten ohne Verlust rasch wiederherzustellen.

- ☒ Regelmäßige Backups der IT Umgebung (Server, Filesystem, DBs, etc.) [Commvault]
- ☒ Handlungsanweisungen für Ausfälle und Störungen (Verhalten im Notfall)
- ☒ USV / NEA Stromunterbrechungstest Server (monatlich)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Datenschutzfreundliche Voreinstellungen § 27 KDG

Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- ☒ vorherige Prüfung der Dokumentation beim Auftragnehmer getroffener Sicherheitsmaßnahmen
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 29 KDG
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 29 KDG)
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn Verpflichtung besteht)
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (oder Rückgabe)
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Kontrolle der Vertragsausführung