Datenschutzprüfung LKI: Ergebnisse

Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz (EKBO)

Das EKD-Datenschutzgesetz ist die für den Bereich der Evangelischen Kirche in Deutschland geltende Datenschutz-Regelung. Die Neufassung ist seit dem 24. Mai 2018 anwendbares Recht. Ziel dieser Prüfung ist die Erhebung und Bewertung des IST-Zustandes gemäß den Anforderungen der DSG-EKD in seiner aktuellen Fassung.

Unsere Tätigkeit in dieser Prüfung erstreckte sich gemäß dieser Planung auf das Prüfungsfeld Datenschutz und beinhaltet keine rechtliche Stellungnahme zur Umsetzung des Datenschutzes. Die Auswahl der Prüfungshandlungen liegt in unserem pflichtgemäßen Ermessen in Abstimmung mit dem örtlich Beauftragten für den Datenschutz. Im Rahmen unserer Prüfung haben wir die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben und Einzelfallprüfungshandlungen beurteilt. Dabei haben wir uns unter anderem ein Verständnis über die eingerichteten Maßnahmen und Prozesse verschafft, Einsicht in relevante Unterlagen genommen sowie die jeweils verantwortlichen Mitarbeiter befragt.

HISOLUTIONS

HiSolutions AG
Bouchéstraße 12
12435 Berlin

info@hisolutions.com
www.hisolutions.com

+49 30 533 289-0
+49 30 533 289-900

Folgende Personen waren in die Prüfung involviert:

Name	Funktion
Franz Schwedler	HiSolutions AG / Durchführung der Datenschutzprüfung
Ergin Kelesoglu	HiSolutions AG / Durchführung der Datenschutzprüfung
Tobias Weiler	HiSolutions AG / Durchführung der Datenschutzprüfung
Tabea Langguth	EKBO / Projektleiterin LKI
Johannes Kellner	EKBO / Örtlich Beauftragter für den Datenschutz
Fabian Kraetschmer	EKBO / Gesamtprojektleitung für die Prüfung

HISOLUTIONS

Gesamtbewertung

Folgende Punkte wurden während der Prüfung des Verarbeitungsverfahrens Landeskirchliches Intranet (LKI) der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz (EKBO) bewertet:

Status	Thema	Kurzeinschätzung
	Prüfung der Auftragsverarbeitungsverträge	Verträge sind strukturell konform, bei VNC sind die TOM sehr unkonkret
	Prüfung Datenschutzinformation	Datenschutzinformationen für Betroffene sind in den Nutzungsbedingungen grundlegend abgebildet, es wird eine Nachbesserung empfohlen
	Prüfung der durchgeführten Datenschutz-Folgenabschätzung (DSFA)	Es wurde eine DSFA auf Basis des PIA Tool durchgeführt. HiS empfiehlt Nachbesserungen die die Qualität der der DSFA weiter erhöhen.
	Verzeichnis von Verarbeitungstätigkeiten (VVT)	Verzeichnis ist vorhanden und entspricht den Anforderungen der DSG-EKD.
	Verfügbarkeitssicherung für das Verfahren	Für die Sicherung der Verfügbarkeit sind Maßnahmen geplant die noch Umsetzungszeit benötigen.
	Sonderpunkt: Risiko besonders sensibler Daten	Es besteht das Risiko eines Uploads der technisch nicht zu verhindern ist. HiS empfiehlt organisatorische Maßnahmen zur Risikoreduktion.

Fazit

Die grundlegende Dokumentation und Prozesse sind für das Verfahren sind vorhanden. An einigen der Dokumente bzw. Maßnahmen sind nacharbeiten notwendig. Die Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz (EKBO) hat die Umsetzung der vorgeschlagenen Maßnahmen zugesagt wodurch sich das Risiko eines Verstoßes auf normal reduziert.

Prüfung der Auftragsverarbeitungsverträge

Status	Einschätzung
	Die EKBO beschäftigt mit dem Betrieb des Intranets drei Dienstleister (Stephanus IT, VNC, Lantec). Nachfolgend wird dargestellt, wie das vorliegende Vertragsverhältnis mit dem jeweiligen Dienstleister bewertet wurde und an welchen Stellen Handlungsempfehlungen bedacht werden sollten.
Empfehlungen:	entfällt

Stephanus IT GmbH

Status	Einschätzung
	Rahmenvertrag und Zusatzvereinbarung zum Rahmenvertrag wurden von HiSolutions geprüft. Im Ergebnis wurde festgestellt, dass keine Auftragsverarbeitung im Sinne des Datenschutzes vorliegt und die Vereinbarungen somit ohne Änderungen fortgesetzt werden können.
Empfehlungen:	entfällt

LANtec Gesellschaft für Datenkommunikation mbH

Status	Einschätzung
	Das Vertragsverhältnis ist aus datenschutzrechtlicher Sicht konform zu DSG-EKD und kann ohne weitere Empfehlungen fortgeführt werden.
Empfehlungen:	entfällt

HISOLUTIONS

VNC – Virtual Network Consult GmbH

Status	Einschätzung
	Das Vertragsverhältnis ist aus datenschutzrechtlicher Sicht konform zu DSG-EKD und mit Übergabe und Darstellung der technischen und organisatorischen Maßnahmen auch für die Verarbeitung von besonderen personenbezogenen Daten ausreichend abgesichert.
Empfehlungen:	Die technischen und organisatorischen Maßnahmen in der vorliegenden Version, sollten in den Vertrag aufgenommen werden. Eine Rücksprache mit dem Dienstleister und ein schriftlicher Vermerk auf dem Dokument, ab wann diese TOM Vertragsbestandteil sind, ist ausreichend.

Datenschutzinformationen

Status	Einschätzung
	Die Datenschutzinformationen für Betroffene sind in den Nutzungsbedingungen grundlegend abgebildet. Eine Information gemäß DSG-EKD wäre so jedoch nicht vollständig möglich.
Empfehlungen:	Es sollten gesonderte Datenschutzinformationen gemäß DSG-EKD erstellt werden. Die gewünschten Awareness Regeln zur Nutzung des Intranets können hier mit aufgenommen werden.

Prüfung der durchgeführten Datenschutz-Folgenabschätzung (DSFA)

Status	Einschätzung
	Die Datenschutzfolgenabschätzung wurde gesichtet und in einer kommentierten Version zurück übergeben. Wie in den Kommentaren bereits empfohlen sollte an den entsprechenden Stellen der Detailgrad erhöht werden um eine belastbare Aussage vorhalten zu können.
Empfehlungen:	Die DSFA sollte an den entsprechenden Stellen nachgearbeitet werden.

HISOLUTIONS

Verfügbarkeitssicherung für das Verfahren

Status	Einschätzung
	Für die Sicherung der Verfügbarkeit sind Maßnahmen geplant die noch Umsetzungszeit benötigen. Es wird ein redundater Server für das Verfahren aufgesetzt. Dieser Server ist bereits vorhanden jedoch noch nicht aufgesetzt. Des Weiteren werden Back-Ups für das System eingeführt.
Empfehlungen:	Umsetzung der geplanten Maßnahmen

Verzeichnis von Verarbeitungstätigkeiten (VVT)

Status	Einschätzung
	Das Verzeichnis von Verarbeitungstätigkeiten ist vorhanden und entspricht den Anforderungen der DSG-EKD.
Empfehlungen:	entfällt

Sonderpunkt:

Risiko besonders sensibler Daten

Status	Einschätzung
	Es besteht das Risiko eines Uploads der technisch nicht zu verhindern ist.
Empfehlungen:	Awareness Regeln erstellen die dem Nutzer sensibilisieren. Einen verschlüsselten Ablageort auf den nur der Nutzer zugreifen kann implementieren.

HISOLUTIONS

Maßnahmenempfehlungen

Empfehlungen:	Umsetzung:
Die technischen und organisatorischen Maßnahmen in der vorliegenden Version, sollten in den Vertrag aufgenommen werden. Eine Rücksprache mit dem Dienstleister und ein schriftlicher Vermerk auf dem Dokument, ab wann diese TOM Vertragsbestandteil sind, ist ausreichend.	Die EKBO wird den Vertrag mit der VNC um die entsprechende Auflistung erweitern.
Es sollten gesonderte Datenschutzinformationen gemäß DSG-EKD erstellt werden. Die gewünschten Awareness Regeln zur Nutzung des Intranets können hier mit aufgenommen werden.	HiSolutions wird die Datenschutzinformationen erstellen.
Die DSFA sollte an den entsprechenden Stellen nachgearbeitet werden.	HiSolutions wird die nacharbeiten durchführen.
Umsetzung der geplanten Maßnahmen	Maßnahmen werden zeitnah umgesetzt.
Awareness Regeln erstellen die dem Nutzer sensibilisieren.	HiSolutions wird die Awareness Regeln erstellen.
Einen verschlüsselten Ablageort auf den nur der Nutzer zugreifen kann implementieren.	Die Möglichkeit einer Implentierung wird mit dem Dienstleiter besprochen. Da es sich hier um eine Back-up Maßnahme handelt wird auf eine feste Zusage verzichtet.

Die Umsetzung der geplanten Maßnahmen wird bis spätestens Mitte 2020 abgeschlossen. Es obliegt dem örtlich Beauftragten der EKBO die Umsetzung Maßnahmen zu prüfen und ggf. Anpassungen zu empfehlen.

Bestätigung der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz (EKBO)

23.10.2019

Datum / Unterschrift

ANHANG

Ampelsymbole

Grün: Normales Risiko

Die vorhandenen Maßnahmen und Dokuemtationen entsprechen der üblichen Praxis und sind den Gefahren für die Rechte und Freiheiten der Betroffenen im allgemeinen angemessen. Das resultierende Risiko für die Organisation bewegt sich im üblichen Rahmen.

Gelb: Erhöhtes Risiko

Die vorhandenen Maßnahmen und Dokuemtationen verfügen über relevante Lücken oder entsprechen nicht mehr dem Stand der Technik. Um eine Absicherung zu erhalten, die der üblichen Praxis entspricht, sind ergänzende Maßnahmen erforderlich. Es ist mit einem erhöhten Risiko für die Rechte und Freiheiten der Betroffenen zu rechnen und damit auch mit einem höheren Bußgeldrisiko.

Rot: Hohes Risiko

Im betrachteten Bereich fehlen zentrale Maßnahmen und Dokumentationen, oder die vorhandenen Maßnahmen bieten keinen ausreichenden Schutz. Zusätzliche Aktivitäten werden dringend empfohlen. Es besteht ein hohes Risiko für die Rechte und Freiheiten der Betroffenen und Bußgelder sowie weitere Sanktionen.