Datenschutz-Folgenabschätzung
gem. Art. 35 DSGVO

Avaya IP OFFICE

Kreisverwaltung Rendsburg-Eckernförde
Kaiserstraße 8
24768 Rendsburg
Deutschland
Telefon 04331 - 202 0
info@kreis-rd.de

Inhaltsverzeichnis

1. Kontext der Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

1.1 Grund für die Durchführung

- Einführung einer neuen Technologie / neuartigen Verarbeitung

1.2 Bezug auf Verarbeitungstätigkeiten

- Keine Angaben

1.3 Akteure und betroffene Personen

Typ des Akteurs	**Kontaktdaten**	**Rolle des Akteurs**	**Standpunkt des Akteurs**
An der Verarbeitung beteiligte Person	Rendsburg-Eckernförde Kaiserstr. 8 24768 Rendsburg	Mitarbeiter Kreis	
Betroffene Person	externe Personen		alle externen Beteiligten an der Nutzung

1.4 Datenschutzbeauftragter

Christian Kock

Kaiserstraße 8

24768 Rendsburg

Deutschland

Telefon 04331 - 202 174

datenschutz@kreis-rd.de

2. Aspekte

2.1 Risikoerhöhende Aspekte

- Keine Fachdienstinterne Abgrenzung. Einsatz im gesamten Kreishaus. Nutzung durch alle Mitarbeiter.

2.2 Risikoreduzierende Aspekte

- Verwaltung von Benutzernamen und Passwörtern sowie Systemzugriffsprotokollierung.
- Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt verarbeiten, wobei keine biometrischen Daten von Betroffenen verarbeitet werden. Die bloße Echtzeitwiedergabe von Gesichtsbildern ist von dieser Ausnahme umfasst.
- Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit angefallenen Dokumente, Abrechnung von Gebühren, Organisation von Großverfahren).
- Dediziertes Rollen- und Rechtekonzept

2.3 Beurteilung der Notwendigkeit

Freiwillige Durchführung der DSFA
Beim Erbringen von VoIP-Dienstleistungen sind die Vorschriften des § 109 I TKG zu beachten. Danach sind Vorkehrungen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten sowie Schutzmaßnahmen gegen unerlaubte Zugriffe zu treffen. Sowohl das Fernmeldegeheimnis als auch der Schutz personenbezogener Daten beschränken sich nicht auf den Schutz gegen Angriffe von außen, sondern die Gesprächsverbindungen und die dabei anfallenden personenbezogenen Daten sind auch gegen unbefugte Kenntnisnahme innerhalb des eigenen Unternehmens oder der eigenen Behörde zu schützen.

3. Beschreibung

3.1 Beschreibung der Zwecke der Verarbeitung

- Durchführung von betriebsinterner Kommunikation
- Durchführung von betriebsexterner Kommunikation

3.2 Art der Daten

- Telefonnummern
- Telefondaten
- IP-Adresse
- Faxnummer
- Name und Vorname interner Mitarbeiter
- Gesprächsinhalte

3.3 Rechtsgrundlage

- Art. 6 Abs. 1 lit. c DSGVO – Rechtmäßigkeit der Verarbeitung (Rechtliche Verpflichtung)

3.4 Regelfristen für die Löschung

- Gesprächsdaten werden nicht gespeichert bzw. aufgezeichnez

3.5 Systematische Beschreibung des Prozesses

Name der Prozessphase	Beschreibung der Prozessphase	Relevante Informationssysteme

3.6 Bestehende Schutzmaßnahmen

- Allgemeine TOM Kreisverwaltung RD-ECK

4. Beurteilung

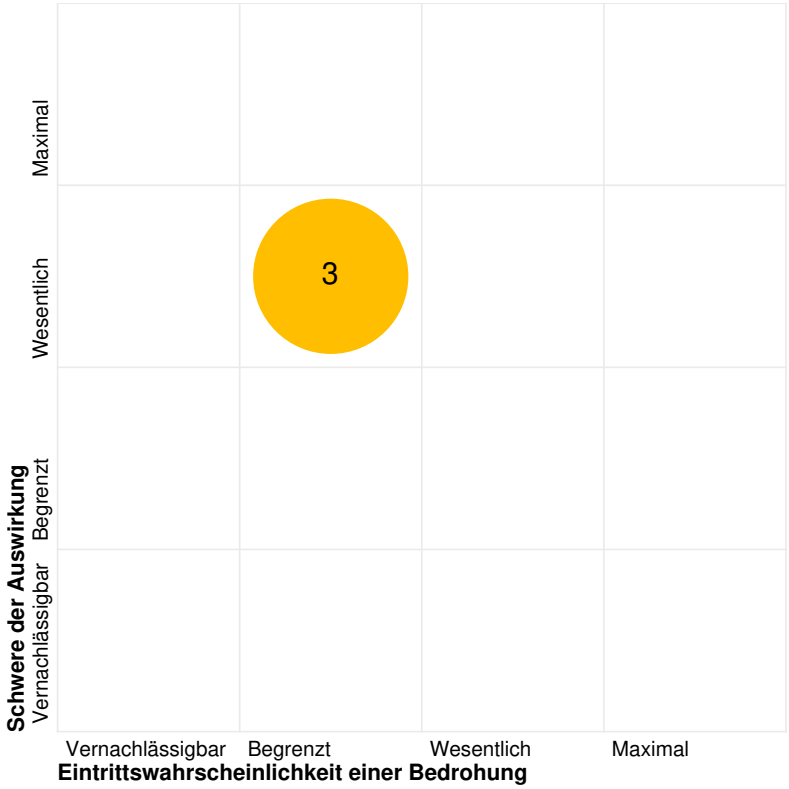
4.1 Beurteilung der Risiken der Verarbeitung

Bezeichnung	Unbefugter Zugriff
Art der Bedrohung	Unbefugter Zugriff
Beschreibung des Risikos	Hacking von extern.
Angreifer bzw. relevante Risikoquellen	▪ Systemintegratoren ▪ externe- und interne "Hacker" (kriminelle Engergie)
Mögliche Schäden (Physisch, materiell, immateriell)	▪ Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile ▪ Finanzielle Verluste ▪ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
Eintrittswahrscheinlichkeit	Begrenzt
Schwere der Auswirkung (Schadenspotenzial für die betroffene Person)	Wesentlich

Bezeichnung	Integrität der Daten
Art der Bedrohung	Unerwünschte Veränderungen der Daten
Beschreibung des Risikos	Zugriffsberechtigte können Daten verändern.
Angreifer bzw. relevante Risikoquellen	▪ externe- und interne "Hacker" (kriminelle Engergie) ▪ Administration durch das IT-Management (techn. Syko)
Mögliche Schäden (Physisch, materiell, immateriell)	▪ Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile ▪ Finanzielle Verluste ▪ Rufschädigung ▪ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
Eintrittswahrscheinlichkeit	Begrenzt
Schwere der Auswirkung (Schadenspotenzial für die betroffene Person)	Wesentlich

Bezeichnung	Unerwünschter Datenverlust
Art der Bedrohung	Verlust von Daten
Beschreibung des Risikos	Internes- und externes Hacking (kriminelle Energie)
Angreifer bzw. relevante Risikoquellen	▪ Administration durch das IT-Management (techn. Syko) ▪ externe- und interne "Hacker" (kriminelle Engergie) ▪ Systemintegratoren
Mögliche Schäden (Physisch, materiell, immateriell)	▪ Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile ▪ Finanzielle Verluste ▪ Rufschädigung ▪ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
Eintrittswahrscheinlichkeit	Begrenzt
Schwere der Auswirkung (Schadenspotenzial für die betroffene Person)	Wesentlich

4.2 Risikokartierung



5. Bewältigung

Bezeichnung	Vertraulichkeit

Schutzziel	Vertraulichkeit
Bezieht sich auf folgendes Risiko	Unbefugter Zugriff
Maßnahmen	▪ Beschränkung des User-eigenen Hardware- und Software-Einsatzes ▪ Change Management ▪ Dokumentation von Verfahren ▪ Einheitlicher Ansprechpartner für Änderungen / Löschungen ▪ Firewalls ▪ Dokumentation ▪ Identity Management ▪ Lösch- und Korrekturkonzept ▪ Non-Disclosure Agreements / Geheimhaltungsvereinbarungen für involvierte Personen ▪ Protokollierung ▪ Protokollierung von Konfigurationsänderungen ▪ Rechte- und Rollenkonzepte mit regelmäßiger Prüfung ▪ Redundanz ▪ Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen ▪ Virenscanner-Einsatz
Beschreibung	Es wirken die zentralen TOMs (technische- und organisatorische Maßnahmen) der Kreisverwaltung
Zuständigkeit für die Umsetzung	IT-Management
Planung der Umsetzung bis	
Status der Umsetzung	Erledigt

Bezeichnung	Integrität der Daten
Schutzziel	Integrität
Bezieht sich auf folgendes Risiko	Integrität der Daten
Maßnahmen	▪ Dokumentation ▪ Dokumentation von Verfahren ▪ Einheitlicher Ansprechpartner für Änderungen / Löschungen ▪ Identity Management ▪ Lösch- und Korrekturkonzept ▪ Log-Dateien aller Anfragen und Server-Aktivitäten ▪ Protokollierung ▪ Protokollierung von Konfigurationsänderungen ▪ Rechte- und Rollenkonzepte mit regelmäßiger Prüfung ▪ Redundanz ▪ Schreibschutz ▪ Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen ▪ Virenscanner-Einsatz
Beschreibung	
Zuständigkeit für die Umsetzung	IT-Management
Planung der Umsetzung bis	
Status der Umsetzung	Erledigt

Bezeichnung	Verfügbarkeit der Daten
Schutzziel	Verfügbarkeit
Bezieht sich auf folgendes Risiko	Unerwünschter Datenverlust
Maßnahmen	▪ Change Management ▪ Dokumentation ▪ Dokumentation von Verfahren ▪ Firewalls ▪ Protokollierung ▪ Rechte- und Rollenkonzepte mit regelmäßiger Prüfung ▪ Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen ▪ Lösch- und Korrekturkonzept ▪ Virenscanner-Einsatz ▪ Systemdokumentation
Beschreibung	
Zuständigkeit für die Umsetzung	IT-Managemenz
Planung der Umsetzung bis	
Status der Umsetzung	Erledigt

6. Bericht

Author	**Hinweise**
Christian Kock (Datenschutzbeauftragter), 11.09.2020	Zusätzlich zu den in den TOM's ergriffenen Maßnahmen wurde eine Dienstvereinbarungen für den Betrieb geschlossen.