



<b>Mitteilungsvorlage</b>	Vorlage-Nr: VO/2017/108	
Federführend: FB 1 Zentrale Dienste	Status: öffentlich	
	Datum: 21.02.2017	
	Ansprechpartner/in: Fiedler, Nina	
	Bearbeiter/in: Fiedler, Nina	
Mitwirkend:	<b>öffentliche Mitteilungsvorlage</b>	
<b>Jahresbericht 2016 Informationssicherheit und Datenschutz</b>		
Beratungsfolge:		
Status	Gremium	Zuständigkeit
Öffentlich	Hauptausschuss	Kenntnisnahme

### 1. Begründung der Nichtöffentlichkeit:

### 2. Sachverhalt:

Nach der Besetzung der Stelle des Informationssicherheitsbeauftragten in 2015 liegt der erste gemeinsame Jahresbericht von behördlichem Datenschutzbeauftragten und Informationssicherheitsbeauftragtem vor und wird dem Hauptausschuss hiermit zur Kenntnis vorgelegt.

Mit der Installation des Informationssicherheitsbeauftragten hat der Kreis die Lücke zwischen IT-Anwendung und Datenschutz geschlossen. Die engen Verflechtungen, die zwischen Informationssicherheit und personenbezogenem Datenschutz notwendig sind, konnten jetzt gebildet werden und haben auch in hohem Maße die Arbeit in 2016 geprägt.

Informationssicherheit und Datenschutz tragen zur Rechtskonformität der Geschäftsprozesse und der Arbeitsfähigkeit auf organisatorisch-technischer Ebene in der Kreisverwaltung bei. Um die operative Ebene so wenig wie möglich zu belasten, wird dabei ein hohes Maß an Aufmerksamkeit darauf gelegt, fertige, sofort umsetzungsfähige Konzepte zu entwickeln und den Organisationseinheiten zur Verfügung zu stellen.

### Finanzielle Auswirkungen:

### Anlage/n:

Jahresbericht 2016 Informationssicherheit und Datenschutz



**Kreis Rendsburg-Eckernförde**  
Informationssicherheitsbeauftragter  
Behördlicher Datenschutzbeauftragter

---

**Jahresbericht 2016**  
**Informationssicherheit und Datenschutz**  
in der  
**Kreisverwaltung Rendsburg-Eckernförde**



Bezeichnung des Dokumentes: Jahresbericht 2016 Informationssicherheit und Datenschutz in der Kreisverwaltung Rendsburg-Eckernförde

Verantwortliche Stelle: Informationssicherheitsbeauftragter (ISB)  
Micha Mark Knierim  
Telefon 04331 / 202-174  
E-Mail: [MichaMark.Knierim@kreis-rd.de](mailto:MichaMark.Knierim@kreis-rd.de)

Behördlicher Datenschutzbeauftragter (DSB)  
Dr. Axel Belz  
Telefon: 04331/202-352  
E-Mail: [axel.belz@kreis-rd.de](mailto:axel.belz@kreis-rd.de)

Dokumentenstatus: intern



## Inhaltsverzeichnis

1	Vorwort .....	4
2	Allgemeines .....	4
3	Ziel des Jahresberichts .....	5
4	Funktion und Aufgaben des Datenschutzbeauftragten .....	6
5	Funktion und Aufgaben des Informationssicherheitsbeauftragten .....	7
6	Ausstattung mit Sachmitteln und Personal .....	8
7	Informationssicherheit und Datenschutz in der Kreisverwaltung 2016 .....	9
7.1	Schutzbedarfsermittlung .....	10
7.2	Verfahrensdokumentation .....	10
7.3	Risikoanalyse .....	10
7.4	Test und Freigabe .....	11
7.5	Personalakten .....	11
7.6	Dienstanweisungen EDV, Internet und E-Mail .....	11
7.7	Revisionssichere Administration und Protokollierung .....	11
7.8	Datenlöschung .....	12
7.9	Active Directory .....	12
7.10	Vorträge zur Sensibilisierung und Information der Beschäftigten .....	12
8	Teilnahme an Arbeitsgruppen/Fortbildung .....	13
9	Ausblick auf das Jahr 2017 .....	13



## 1 Vorwort

Dies ist der erste gemeinsame Jahresbericht von behördlichem Datenschutzbeauftragten und Informationssicherheitsbeauftragtem. Bis dahin lag der eindeutige Schwerpunkt der vorangegangenen Jahresberichte auf dem Datenschutz, was hauptsächlich der Tatsache geschuldet war, dass die Stelle des Informationssicherheitsbeauftragten erst im Laufe des Jahres 2015 eingerichtet und besetzt worden ist.

Mit der Installation des Informationssicherheitsbeauftragten hat der Kreis die Lücke zwischen IT-Anwendung und Datenschutz geschlossen. Die engen Verflechtungen, die zwischen Informationssicherheit und personenbezogenem Datenschutz notwendig sind, konnten jetzt gebildet werden und haben auch in hohem Maße die Arbeit in 2016 geprägt.

Die verschiedensten Informations- und Datenschutzprozesse müssen durch das Sicherheitsmanagement ständig weiter ausgestaltet und ggf. initiiert werden. Dabei sind generell die Verhältnismäßigkeit der Mittel und die Arbeitsfähigkeit der Kreisverwaltung zu beachten und sicherzustellen.

Informationssicherheit und Datenschutz tragen zur Rechtskonformität der Geschäftsprozesse und der Arbeitsfähigkeit auf organisatorisch-technischer Ebene in der Kreisverwaltung bei. Um die operative Ebene so wenig wie möglich zu belasten, wird dabei ein hohes Maß an Aufmerksamkeit darauf gelegt, fertige, sofort umsetzungsfähige Konzepte zu entwickeln und den Organisationseinheiten zur Verfügung zu stellen.

## 2 Allgemeines

Die informationstechnische und –organisatorische Entwicklung hat im abgelaufenen Jahr weiter Fahrt aufgenommen. Die Möglichkeiten werden immer komplexer und damit für den Einzelnen immer undurchschaubarer. Wenn in 2016 ständig von Hackerangriffen, Ransomware und Social-Engineering zu lesen war, so sind diese kriminellen Energien auch und zuerst auf die wachsenden Anforderungen bei gleichzeitig abnehmender Transparenz der Informations- und Datenverarbeitung zurückzuführen.

Die Gefahr geht jedoch nicht – nur – von außen aus. Je anspruchsvoller eine Aufgabe ist – und die Informationssicherheit und der Datenschutz sind anspruchsvolle Aufgaben – desto mehr muss das Augenmerk intern auf diese Aufgaben gerichtet sein.



Dabei hat die Erfahrung gezeigt, dass technische Maßnahmen nur bis zu einem gewissen Grad die Informationssicherheit und den Datenschutz verbessern können. Ein großer Teil, der zur verbesserten Sicherheit beitragen kann und auch muss, ist der Faktor Mensch.

Jedes Nachlassen der Konzentration, jede Nachlässigkeit bei der Anwendung von Sicherheitsmaßnahmen und jedes Nicht-ernst-nehmen von Regelungen erleichtert Angreifern den Zugriff auf Informationen und Daten.

Deshalb ist es von nicht zu unterschätzender Bedeutung, diese Themenfelder permanent im Blickfeld zu haben. Um dies zu erreichen ist es wichtig ein Bewusstsein für Informationssicherheit und Datenschutz bei den Mitarbeitern zu schaffen. Hierfür hat sich der Begriff der „Awareness“ (im Sinne von Sensibilisierung) etabliert.

Es darf auch nicht der Eindruck entstehen, dass die Daten der Kreisverwaltung für Dritte uninteressant oder irrelevant seien. Ein derartig falsches Verständnis würde unmittelbar zu einer Fehleinschätzung und damit zu einem Nicht-wichtig-nehmen von Informationssicherheit und Datenschutz führen.

Motive von Hackern sind vielfältig. Meist verschaffen sie sich unberechtigten Zugriff auf fremde Computersysteme, um die Kontrolle über das System zu übernehmen und die Daten zu verschlüsseln oder Daten zu stehlen. Sodann werden die gestohlenen Informationen bzw. die Entschlüsselung gegen Lösegeld angeboten.

Eine verlässliche Informationssicherheit und ein aktiver Datenschutz sind daher unumgänglich und für eine Kreisverwaltung, die das Bürgerinteresse in den Mittelpunkt ihrer Tätigkeit gestellt hat der Gradmesser für die Ernsthaftigkeit dieses Zieles.

Daher sollte trotz der aktuellen politischen Diskussion um den Umfang von Informationssicherheit und Datenschutz angesichts der Bedrohungen von außen stets das Augenmerk insbesondere der Führungskräfte auch darauf gerichtet sein, sich aktiv für die Informationssicherheit und den Datenschutz einzusetzen und deren Einhaltung bei den Beschäftigten einzufordern.

### **3 Ziel des Jahresberichts**

Dieser Bericht dient dazu, den verantwortlichen Stellen in der Kreisverwaltung und gegebenenfalls auch den Mitarbeitenden einen Überblick über die Entwicklungen und den Stand der Dinge im betrieblichen Datenschutz und der Informationssicherheit zu geben.

Der Bericht gilt für den Zeitraum vom 01. Januar 2016 bis zum 31. Dezember 2016.



Es ist das Ziel des Berichtes, die Ereignisse und Aktivitäten des abgelaufenen Jahres schriftlich zu erfassen und gleichzeitig auf Planungen für die kommende Periode hinzuweisen. Dabei soll auch auf die Themen aufmerksam gemacht werden, die (noch) nicht oder nicht optimal bewältigt wurden, um allen Beteiligten die Möglichkeit zu geben, an einer Verbesserung mitzuwirken.

## **4 Funktion und Aufgaben des Datenschutzbeauftragten**

Der behördliche Datenschutzbeauftragte ist unmittelbar dem Landrat unterstellt.

Er überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der datenverarbeitenden Stelle. Er hat insbesondere

- auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken
- Richtlinien und Regelungen, die den Datenschutz der Kreisverwaltung betreffen, zu erstellen bzw. anzuregen
- die Beschäftigten der datenverarbeitenden Stelle mit den Bestimmungen des Landesdatenschutzgesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen
- die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken
- das Verzeichnisse der Verfahren zu führen und zur Einsicht bereitzuhalten
- die Verfahrensakten zu prüfen
- die Vorabkontrolle durchzuführen
- regelmäßig den Landrat über den aktuellen Stand des Datenschutzes zu unterrichten.

Darüber hinaus gilt:

- Beschäftigte und Betroffene können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden
- er darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen



- in Zweifelsfällen hat er das Unabhängige Landeszentrum für Datenschutz zu hören
- die datenverarbeitende Stelle ist verpflichtet, ihn bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere Auskunft zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen; besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen. Ihm ist der Zutritt zu allen Diensträumen zu gewähren.
- er bildet zusammen mit dem Informationssicherheitsbeauftragten das integrierte Sicherheitsmanagementsystem des Kreises Rendsburg- Eckernförde (ISMS Kreis RD-Eck).

## **5 Funktion und Aufgaben des Informationssicherheitsbeauftragten**

Der Informationssicherheitsbeauftragte ist zuständig für die Belange der Informationssicherheit. Er unterstützt die Leitungsebene bei deren Aufgaben bezüglich der Informationssicherheit und ist dahingehend beratend tätig. Er

- bildet zusammen mit dem Datenschutzbeauftragten das integrierte Sicherheitsmanagementsystem des Kreises Rendsburg-Eckernförde (ISMS Kreis RD-ECK)
- stimmt die Informationssicherheitsziele mit den Zielen der Behörde ab
- initiiert den Aufbau, Betrieb und die Weiterentwicklung der Informationssicherheitsorganisation innerhalb der Behörde
- erstellt Richtlinien und Regelungen, die die Informationssicherheit der Kreisverwaltung betreffen
- berät die Leitungsebene in allen Fragen der Informationssicherheit
- berichtet relevante, die Informationssicherheit betreffende Vorkommnisse an die Leitungsebene
- berichtet der Leitungsebene regelmäßig über den aktuellen Stand der Informationssicherheit
- stellt den notwendigen Informationsfluss für das ISMS sicher (z. B. durch Berichtswesen, Dokumentation)



- stellt sicher, dass die Informationssicherheitsmaßnahmen inklusive der Zugriffsregelungen aktuell, aussagekräftig und nachvollziehbar dokumentiert werden
- initiiert und kontrolliert die Umsetzung von Informationssicherheitsmaßnahmen
- koordiniert zielgruppenorientierte Sensibilisierungs- und Schulungsmaßnahmen zum Thema Informationssicherheit oder führt diese selbst durch
- plant und konzipiert die Notfallvorsorge
- bindet alle Mitarbeiterinnen und Mitarbeiter der Kreisverwaltung in den Informationssicherheitsprozess und die Notfallvorsorge ein
- kategorisiert Informationssicherheitsprobleme/-Vorfälle und übernimmt die Leitung der Analyse, sowie deren Nachbearbeitung
- arbeitet mit anderen Informationssicherheitsbeauftragten auf Kommunal-, Landes- und Bundesebene zusammen (z. B. SiKoSH).

## **6 Ausstattung mit Sachmitteln und Personal**

Sowohl der behördliche Datenschutzbeauftragte als auch der Informationssicherheitsbeauftragte sind unmittelbar der Leitung der Kreisverwaltung unterstellt. Sie sind bei der Ausübung des Amtes weisungsfrei und dürfen wegen der Wahrnehmung des Amtes nicht benachteiligt werden. Sie sind zur Erfüllung der Aufgaben des Amtes im erforderlichen Umfang freizustellen und mit den notwendigen Mitteln auszustatten. Seit dem 01. April 2013 ist die Stelle des behördlichen Datenschutzbeauftragten als Vollzeitstelle ausgestaltet und entsprechend besetzt und bietet damit ausreichend Ressourcen, um den Anforderungen der Aufgabe gerecht werden zu können. Für 2016 wurde (wie 2015) ein Budget von 900,- € bereitgestellt, das für Fortbildungsmaßnahmen und Erwerb von Fachliteratur genutzt wurde.

Die Stelle des Informationssicherheitsbeauftragten ist seit dem 01.09.2015 in Vollzeit besetzt. Ein besonderes Sachmittelbudget für 2016 konnte im Haushalt hierfür nicht mehr veranschlagt werden.

Die Sachmittelausstattung war in 2016 ausreichend.

Mit der Ausgestaltung als Vollzeitstellen zeigt der Kreis seinen Willen, die Verantwortung für die Informationssicherheit und die personenbezogenen Daten seiner Bürgerinnen und Bürger ernst zu nehmen und durch entsprechende Schutzmaßnahmen zu gewährleisten.



## **7 Informationssicherheit und Datenschutz in der Kreisverwaltung 2016**

Die Themen Informationssicherheit und Datenschutz sind prozessual geprägte Themenfelder. Es bedarf dahingehend immer wiederkehrender Zyklen aus Planung, Abstimmung, Umsetzung, Kontrolle und Verbesserung. Zudem ist die rechtzeitige Einbindung des Informationssicherheits- und des Datenschutzbeauftragten in anstehende Projekte, Entscheidungen und bestehende Prozesse unabdingbare Voraussetzung für die Schaffung effektiver Sicherheits- und Schutzmaßnahmen.

Der Aufbau eines umfassenden Informationssicherheits- und Datenschutzmanagementsystems beträgt im Durchschnitt 5-7 Jahre. Wir stehen insbesondere im Bereich der Informationssicherheit am Anfang. Das bedeutet aber nicht, dass es bislang keine entsprechenden Prozesse, Leitlinien und Maßnahmen gibt, die der Schutzbedürftigkeit der Informationssysteme nicht gerecht werden. Vielmehr gibt es bereits viele Bereiche, in denen aus Sicht der Informationssicherheit und des Datenschutzes sinnvolle, effektive und praxisorientierte Lösungen etabliert sind. Diese gilt es im Zuge einer Ist-Analyse zu identifizieren, rechtskonform zu optimieren und zu dokumentieren.

Es geht folglich um viele Einzelthemen, die im Spannungsfeld von Notwendigkeit, Handhabbarkeit und Verhältnismäßigkeit stehen.

Das vergangene Jahr war das erste, das vollständig auch das Thema Informationssicherheit im Fokus hatte. Deshalb war auch die Jahresplanung zu den Themen Informationssicherheit und Datenschutz von einer großen Schnittmenge geprägt und wurde gemeinsam verfasst. Informationssicherheit ist heute vom Datenschutz fast nicht mehr zu trennen und dies gilt umgekehrt genauso. Dabei entwickeln sich immer komplexer werdende technisch gestützte Abläufe. Im Fokus stehen elektronische Verfahren und organisatorische Prozesse, ohne deren Unterstützung die meisten betrieblichen Abläufe einer Behörde nicht mehr aufrechterhalten werden könnten.

Im Berichtsjahr lagen die datenschutzbezogenen Schwerpunkte im operativen Bereich. Es gab zahlreiche Anfragen zum IZG und zur Auskunftserteilung, insbesondere nach dem SGB.

Bei der Einführung neuer Verfahren wurde der Datenschutz regelmäßig beteiligt. Die erforderlichen Verfahrensdokumentationen wurden erstellt.

Es waren Ortstermine im Zusammenhang mit der Einrichtung eines alternierenden Telearbeitsplatzes wahrzunehmen.

Routinemäßig begann die Überprüfung der bestehenden Verfahrensakten nach zwei Jahren. Als eindeutiger Schwachpunkt zeigte sich dabei die unterlassene Freigabeerklärung nach Programmänderungen. Den aktenführenden Stellen wurde das korrekte Vorgehen erläutert und es wurde um zukünftige Beachtung gebeten.



Die „Dienstanweisung zur datenschutzkonformen Behandlung von Akten“ wurde in Kraft gesetzt.

Die Sensibilität für das Thema Datenschutz ist bei den Führungskräften und Mitarbeitern in 2016 weiter gewachsen. Dies ergibt sich aus der hohen Anzahl von Anfragen ebenso, wie aus deren Qualität, aber auch daraus, dass die Reaktionszeiten deutlich geringer waren als in den Vorjahren. Die Zusammenarbeit mit den einzelnen Organisationseinheiten kann ohne Einschränkung als gut und sehr gut bezeichnet werden. Das Vertrauen in die Arbeit von Informationssicherheits- und Datenschutzbeauftragtem ist erkennbar gewachsen, die Notwendigkeit dieser Aufgabengebiete wird akzeptiert. Die Aufgabe von Informationssicherheits- und Datenschutzbeauftragtem wird als Unterstützungsleistung anerkannt und nicht als notwendiges Übel, welches im Zweifel rationelles Arbeiten erschwert.

Neben dem Tagesgeschäft war die Arbeit von Informationssicherheitsbeauftragtem und Datenschutzbeauftragtem von den Aufgaben geprägt, die sich aus der Jahresplanung 2016 ergaben. Dabei handelt es sich um die folgenden Themenbereiche (7.1 – 7.10).

## **7.1 Schutzbedarfsermittlung**

Es wurden insgesamt 49 Fachverfahren überprüft und nach der Methodik des BSI-Grundschutzes bei ihnen der Schutzbedarf ermittelt. Die von Informationssicherheitsbeauftragtem und Datenschutzbeauftragtem vorgeschlagenen Einschätzungen wurden in nahezu sämtlichen Fällen von den verantwortlichen Leitungskräften bestätigt. In einem Falle wurde der Bedarf von „normal“ auf „hoch“ korrigiert. Insgesamt wurden 24 Verfahren als „normal“ und 25 Verfahren mit dem Schutzbedarf „hoch“ eingestuft.

Der hohe Schutzbedarf ergab sich hauptsächlich aus Gründen der Verfügbarkeit oder der besonderen Schutzbedürftigkeit der Daten nach § 11 Absatz 3 LDSG.

## **7.2 Verfahrensdokumentation**

Das bisherige Muster wurde überarbeitet und dabei an die Bedürfnisse der Kreisverwaltung angepasst. Die im Laufe des Jahres neu zu erstellenden Verzeichnisse sind bereits in der neuen Form aufgebaut worden. Das Muster ist im Intranet verfügbar.

## **7.3 Risikoanalyse**

Für alle Verfahren mit hohem Schutzbedarf, in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit, schließt sich die Risikoanalyse an.



Dabei muss bewertet werden, welche Gefährdungen (gem. BSI Grundschutz-Gefährdungskatalog) für die Kreisverwaltung bestehen und wie diese für die Informationsverarbeitung minimiert werden können. Daraus resultieren zusätzliche Maßnahmen, die noch einmal der Verhältnismäßigkeit und den bestehenden organisatorischen Regelungen gegenüber zu stellen sind. Aufgrund der Komplexität dieses Themas, reicht die Umsetzung bis weit ins Jahr 2017 hinein.

#### **7.4 Test und Freigabe**

Es liegt eine Arbeitshilfe „Vorgehen bei Test und Freigabe für die Kreisverwaltung Rendsburg-Eckernförde“ vor. Diese wurde am 24.05.2016 per E-Mail den Fachverantwortlichen zugesandt und ist auch im Intranet abrufbar.

#### **7.5 Personalakten**

Der Umgang mit Personalakten wirft immer wieder Fragen auf, die insbesondere den Datenschutz betreffen. Dabei geht es häufig um das Thema von doppelter Aktenführung und (Einsichts-)rechten der Führungskräfte. Um hier für Klarheit zu sorgen, wurde eine „Information für die Führungskräfte zum Umgang mit Personaldaten- und akten“ erstellt und mit dem zuständigen Fachdienst 1.1 (Personal, Organisation und allgemeine Dienste) abgestimmt.

#### **7.6 Dienstanweisungen EDV, Internet und E-Mail**

Die Dienstanweisungen EDV und Internet & E-Mail sind grundlegend überarbeitet worden. Beide neue Dienstanweisungen sind im Intranet der Kreisverwaltung abrufbar.

#### **7.7 Revisionssichere Administration und Protokollierung**

Laut § 6 Abs. 2 LDSG dürfen nur berechtigte Personen auf Daten zugreifen. Des Weiteren sind diese Zugriffe zu protokollieren und zu kontrollieren.

Ein Administrator verfügt über weitreichendere Zugriffsmöglichkeiten als jeder andere Nutzer und steht im Falle von Missbrauch und unkontrolliertem Datenabfluss automatisch unter Generalverdacht. Nicht zuletzt deshalb ist es wichtig, eine revisionssichere Administration zu gewährleisten.

Die durchgeführte Schwachstellenanalyse zu den jetzigen Administratorenrechten hat ergeben, dass eine Revisionssicherheit zurzeit nicht besteht. Es hat sich gezeigt, dass der Regelungsaufwand erheblich höher ist, als veranschlagt. Zudem ist deutlich



geworden, dass eine revisionssichere Administration stark von einem Protokollierungsserverkonzept abhängig ist. Deshalb wurde das Thema Protokollierung als vorrangig eingestuft.

Die Unterzeichner haben dazu ein Projekt in Zusammenarbeit mit dem ULD initiiert. Vor dem Projektstart in 2017 gab es in 2016 ein Vorabgespräch. An diesem nahm die spätere Projektlenkungsgruppe und die Datenschutzbeauftragte des Landes Schleswig-Holstein teil.

## **7.8 Datenlöschung**

Die rechtskonforme Löschung personenbezogener Daten ist eine tragende Säule des Datenschutzes. Inwieweit dem Grundsatz der Datenlöschung Rechnung getragen wird, sollte durch die Analyse festgestellt werden.

Die Untersuchung hat ergeben, dass es für die Löschung von Daten keinerlei kreisinterne Regelung gibt, die die gesetzliche Löschungspflicht konkretisiert. Mangels Regelung gibt es auch keine einheitliche Vorgehensweise. Selbst die gesetzlichen bzw. definierten Aufbewahrungsfristen werden nicht konsequent beachtet.

## **7.9 Active Directory**

Active Directory ist ein von Microsoft entwickelter Verzeichnisdienst, in dem unter anderem alle Benutzerkonten der Mitarbeiterinnen und Mitarbeiter geführt werden. Verwaltungsaufgaben innerhalb des Kreisnetzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können durch den Einsatz eines Verzeichnisdienstes effizienter durchgeführt werden. Er ist eines der zentralen und damit auch sensiblen Elemente in der behördlichen IT-Landschaft der Kreisverwaltung. Nicht zuletzt deshalb ist er gesondert zu betrachten und abzusichern.

Für den erfolgreichen Betrieb eines Active Directorys ist eine Reihe von Sicherheitsmaßnahmen umzusetzen.

Die Voraussetzungen für eine stichprobenartige Revision der Einhaltung datenschutzrechtlicher Vorgaben und informationssicherheitsseitiger Notwendigkeiten wurden geschaffen, die Revision wird in 2017 durchgeführt.

## **7.10 Vorträge zur Sensibilisierung und Information der Beschäftigten**

Die in der Jahresplanung vorgesehenen Vorträge wurden planmäßig durchgeführt. Dabei handelte es sich um die Themen:



- Grundlagen der Informationssicherheit
- Das ABC des Datenschutzes
- Das Informationszugangsgesetz Schleswig-Holstein.

Die Veranstaltungen sind von den Besuchern gut angenommen worden. Das zeigte sich nicht nur an den Teilnehmerzahlen, sondern auch an vielen positiven Reaktionen auf diese Themen.

Außerdem wurde der Jahresbericht 2015 den Führungskräften der Kreisverwaltung in einem Vortrag erläutert.

## **8 Teilnahme an Arbeitsgruppen/Fortbildung**

Der Informationssicherheitsbeauftragte und der Datenschutzbeauftragte sind Mitglieder verschiedener Arbeitsgruppen. Insbesondere sind dabei „SiKoSH“ (Sicherheit für Kommunen in Schleswig-Holstein), „Modernisierung des BSI-Grundschutzes“ (Bonn/Berlin) und der „Arbeitskreis der behördlichen Datenschutzbeauftragten der Kreise“ zu nennen.

Sowohl Informationssicherheitsbeauftragter als auch Datenschutzbeauftragter haben an den Sitzungen ihrer Arbeitsgruppen regelmäßig teilgenommen.

Der Datenschutzbeauftragte hat an folgenden Fortbildungsmaßnahmen teilgenommen:

- Grundlagen der Dokumentation nach DSVO
- Datenschutzlecks in Behörden und Unternehmen.

Der Informationssicherheitsbeauftragte hat folgende Maßnahmen besucht:

- Sommerakademie des ULD
- im Rahmen des SiKoSH-Projekts einen zweitägigen Awareness Workshop
- eine Fortbildung zum Thema IT-Recht.

## **9 Ausblick auf das Jahr 2017**

Außerhalb der Kreisverwaltung wird das Jahr 2017 geprägt sein von einer ständig zunehmenden Menge an Informationen in Bezug auf die EU Datenschutzgrundverordnung, die im Mai 2018 in nationales Recht transferiert werden muss. Wenngleich sich hieraus für die Kreisverwaltung im nächsten Jahr voraussichtlich noch keine akuten Handlungsverpflichtungen ergeben werden, so muss die Entwicklung dennoch verfolgt werden, um rechtzeitig erkennbare und notwendig werdende Änderungen planen, vorbereiten und durchführen zu können.



Es gehört zu den Aufgaben von Informationssicherheitsbeauftragtem und Datenschutzbeauftragtem, auf die Umsetzung der Anpassungen der nationalen Regelungen hinzuwirken.

Intern kommt dem Projekt „revisionssichere Protokollierung“, das Informationssicherheitsbeauftragter und der Datenschutzbeauftragter gemeinsam mit dem ULD durchführen, die größtmögliche Bedeutung zu. Ziel dieses Projektes ist es, über einen Protokollierungsserver die revisionssichere Protokollierung zu gewährleisten.

Diese Aufgabe stellt die bisher umfangreichste und anspruchsvollste Herausforderung an die Unterzeichner dar. Es gibt keine Blaupause, so dass Vieles im Wege von „Versuch und Irrtum“ ausprobiert werden muss. Das Projekt soll ca. zwei Jahre dauern.

Außerdem wird die Risikoanalyse einen breiten Raum einnehmen. Dabei muss bewertet werden, welche Gefährdungen (gem. BSI Grundschutz-Gefährdungskatalog) für die Kreisverwaltung bestehen und wie diese für die Informationsverarbeitung minimiert werden können.

Neben weiteren Themen wie Notfallmanagement, Löschkonzept, Personalakten und Rechtevergabe wird im Rahmen des Sicherheits- und Datenschutzmanagements das BSI-Tool Verinice zum Einsatz kommen, mit dessen Hilfe der hiesige IT-Verbund und die Datenschutzregelungen nachvollziehbarer und hinsichtlich umgesetzter Maßnahmen und Anforderungen transparenter gemacht werden können.

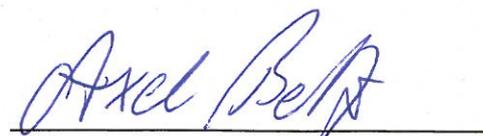
Schließlich wird es auch in 2017 wieder Veranstaltungen in Form von Vorträgen zu den Themen Datenschutz und Informationssicherheit geben. Daneben soll eine Reihe von Awareness-Maßnahmen die Sensibilisierung auf die anstehenden Themen erhöhen.

Die genannten Herausforderungen machen auch einen höheren Ressourceneinsatz erforderlich, so dass das Budget im Haushalt 2017 deutlich erhöht werden musste. Der Zeitplan ist der anschließenden Graphik zu entnehmen.

Der aktuelle Sachstand ist dem Landrat vierteljährlich zu berichten.

Rendsburg, 1. Februar 2017

  
\_\_\_\_\_  
Micha Mark Knierim  
Informationssicherheitsbeauftragter

  
\_\_\_\_\_  
Dr. Axel Belz  
Datenschutzbeauftragter