Ordnung Informationssicherheit und Datenschutz im Generalvikariat des Erzbistums Köln

Festlegung der grundlegenden Ziele, der organisatorischen und strategischen Maßgaben zur Umsetzung von Informationssicherheit und Datenschutz

Version: 1.0.

vom: 14.04.2014

Inhalt

1. Leitideen des Informationssicherheits- und Datenschutzmanagements

Das Generalvikariat des Erzbistums Köln verwaltet wesentliche Daten des Bistums und ist dazu ebenso auf die Sicherheit dieser Daten angewiesen, wie auch zur Wahrung der Anforderungen des kirchlichen Datenschutzes verpflichtet. Neben der Verfügbarkeit und Vertraulichkeit sind in den meisten Fällen auch die Integrität und Authentizität von Informationen für die Aufrechterhaltung unserer Dienst- und Geschäftstätigkeit von größter Wichtigkeit.

Die Daten aus Gemeinden und Einrichtungen des Erzbistums Köln sind nicht nur innerhalb der Hoheit des Generalvikariats zu schützen. Wir sind daher bestrebt, unsere eigenen Strukturen und Prozesse so zu optimieren, dass ein angemessenes Informationssicherheits- und Datenschutzniveau erreicht wird, während wir uns zugleich auch außerhalb unseres Hoheitsbereiches für angemessene Maßnahmen stark machen wollen.

Nach Maßgabe dieser Ordnung ist jede Organisationseinheit und Einrichtung des EGVs sowie jede Stelle, die Daten des EGVs verarbeitet oder auf Systeme des EGVs zugreift, für die Sicherheit und den angemessenen Schutz der Informationen verantwortlich. Jeder Mitarbeitende muss sich daher der Notwendigkeit von Datenschutz und Informationssicherheit bewusst sein und entsprechend handeln.
Diese Maßnahmen sind nicht nur gesetzlich vorgeschrieben, sondern auch Teil unserer Verpflichtungen gegenüber dem Erzbistum sowie den Gemeinden, Kirchenmitgliedern und der Öffentlichkeit.
Sicherheitsbewusstsein ist durch folgendes Verhalten gekennzeichnet:

- Erkennen, dass effektive Sicherheit ein kritisches und wesentliches Element der Dienst- und Geschäftstätigkeit im EGV ist.
- Stets vorhandenes Sicherheitsbewusstsein bei allen täglich anfallenden Aktivitäten beweisen.
- Persönliche Verantwortlichkeit für proaktive Maßnahmen in Bezug auf sämtliche Risiken für Mitarbeitende, Informationen, Vermögenswerte und die Fortführung der Dienst- und Geschäftstätigkeit im Notfall übernehmen.

Personenbezogene Daten müssen so geschützt werden, dass

- Daten nur innerhalb der Zweckbindung verarbeitet werden,
- Daten nicht unerlaubt verarbeitet werden können,
- Betroffenenrechte gewährleistet werden können,
- die Verarbeitung der personenbezogenen Daten transparent und nachvollziehbar ist,
- gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllt werden können.

2. Geltungsbereich

Diese Ordnung und das Informationssicherheits- und Datenschutzmanagement sind für jeden, der im oder für das EGV arbeitet (interne Mitarbeitende, Berater und Zulieferer) sowie für alle Stellen und Mitarbeitende, die auf Daten oder Systeme des EGVs zugreifen, verpflichtend.

Betrachtet werden sämtliche Informationen aus

- Daten
- Anwendungen
- Systemen
- Kommunikationsvorgängen
- organisatorischen Abläufen

3. Ziel des Informationssicherheits- und Datenschutzmanagements

Der Aufbau und Betrieb eines Informationssicherheits- und Datenschutzmanagements im EGV verfolgt das Ziel, die Daten ihrer jeweiligen Wichtigkeit nach vor unbefugtem Zugriff, Verfälschung und Zerstörung zu bewahren.

Dies soll

- zum einen durch entsprechende Maßnahmen zur Gewährleistung und Aufrechterhaltung der Informationssicherheit und des Datengeheimnisses,
- zum anderen durch geeignete Maßnahmen zur Wiederherstellung der Informationen im Falle eines unausweichlichen Verlustes

bewerkstelligt werden.

4. Geregelte Bereiche

Das EGV betrachtet vorausschauendes Informationssicherheits- und Datenschutzmanagement als eine wichtige Führungsaufgabe, die sowohl die Entwicklung der Leitideen als auch die Verantwortung für die Informationssicherheits- und Datenschutzpolitik umfasst. Ziel ist, den IT-Einsatz und die elektronische sowie manuelle Datenverarbeitung jeglicher Art so zu lenken und kontinuierlich weiterzuentwickeln, dass potenzielle Risiken eingeschätzt und kontrolliert werden können. Dieser ganzheitliche Ansatz gewährleistet, dass die Anforderungen der einzelnen Abteilungen und deren Wechselbeziehungen berücksichtigt werden.

In Anlehnung an den Sicherheitsstandards ISO/IEC 27001:2005 müssen die folgenden Organisationsbereiche geregelt werden:

- Informationssicherheits- und Datenschutzpolitik und Organisation der Sicherheit
- Management organisationseigener Werte
- Personelle Sicherheit
- Physikalische und umgebungsbezogene Sicherheit
- Management des Betriebes und der Kommunikation
- Zugangskontrolle
- Beschaffung, Entwicklung und Wartung von Informationssystemen
- Umgang mit Informationssicherheitsvorfällen
- Fortführung des Dienst- und Geschäftsbetriebes bei Vorfällen
- Datenschutz-Management und Management der Einhaltung vertraglicher, branchenüblicher und gesetzlicher Verpflichtungen (Compliance)

Diese Ordnung dient zur Feststellung der Zielsetzungen der Informationssicherheits- und Datenschutzpolitik sowie der Organisation der Sicherheit.

Damit das EGV gezielt Werte schützen kann, sind ein umfassendes Werte-Inventar und eine Zuweisung von Verantwortlichkeiten für Werte zwingend erforderlich. Zudem müssen die Informationswerte entsprechend ihren Vertraulichkeitsstufen angemessen gekennzeichnet und gehandhabt werden.

Die Mitarbeitenden des EGVs sind die Träger des Informationssicherheits- und Datenschutzmanagements und als solche unter besonderer Berücksichtigung der Sicherheitsanforderungen im Unternehmen auszuwählen sowie regelmäßig und systematisch zu schulen. Auch beim Ausscheiden von Mitarbeitenden muss zielgerichtet und schnell verfahren werden, um eventuelle Sicherheitslücken unmittelbar zu schließen. Dies gilt auch für Fremd-Mitarbeitende, die in den Räumlichkeiten und mit den Systemen des EGVs arbeiten.

Zutritt zu den Räumlichkeiten an allen Standorten und damit Zutritt zu den informationsverarbeitenden Systemen des EGVs ist unter besonderer Berücksichtigung der Philosophie des „offenen Hauses" durch gesonderte Maßnahmen für definierte schutzwürdige Bereiche zu regeln.

Im Sinne eines Qualitätsmanagements sind die Kernverfahren des EGVs zu dokumentieren und unter Informationsicherheits- und Datenschutzgesichtspunkten zu optimieren. Schwerpunkte werden auf Kommunikations-, Datensicherungs- und Netzwerkprozesse gelegt.

Das Zugriffsmanagement muss hinsichtlich der Netzwerke, Applikationen und Systeme Dienst- und Informationssicherheitsanforderungen vereinen und die unterschiedlichen Modalitäten des Arbeitens in Betracht ziehen (mobile Arbeit, Telearbeit,...). Die Verantwortung der Anwender für die Sicherheit der Zugänge ist zu stärken. Um frühzeitig ein einheitliches und angemessenes Informationssicherheits- und Datenschutzniveau anzustreben sind die Anforderungen insbesondere in den Beschaffungs-, Wartungs- und Entwicklungsprozessen des EGV zu berücksichtigen.

Einen wesentlichen Schwerpunkt bildet dabei die Vereinheitlichung und Optimierung von Eigenentwicklungen unter Informationssicherheits- und Datenschutzaspekten.

Der Umgang mit Sicherheitsvorfällen muss sowohl das Erkennen und Behandeln von Risiken, als auch die Nachhaltung und Überprüfung korrektiver Maßnahmen berücksichtigen. Aus Fehlern soll systematisch gelernt werden.

Spezielle Beachtung wird der Fortführung des Dienst- und Geschäftsbetriebes zugemessen: auch unter erschwerten Bedingungen von Stör- oder Notfällen muss dieser jederzeit aufrechterhalten werden können. Die hohen Anforderungen an die Verfügbarkeit der IT-Infrastruktur müssen sich in deren Organisation und Aufbau wiederfinden.

Essentiell für das Informationssicherheits- und Datenschutzmanagement im EGV sind die Vorgaben aus der KDO. Diese Vorgaben gelten auch für alle angeschlossenen Einrichtungen sowie sonstige Partner im Sinne des Geltungsbereiches (gem. Kapitel " 2. Geltungsbereich"). Für die Überwachung der Datenverarbeitung und die Überwachung der Einhaltung der gesetzlichen Vorgaben ist der betriebliche Datenschutzbeauftragte (bDSB) zuständig. Die Zusammenarbeit des bDSB mit anderen (betrieblichen) Datenschutzbeauftragten zur Gewährleistung eines hohen Datenschutzniveaus ist ausdrücklich erwünscht. Als zentrale Kontrollinstanz ist hier die Diözesandatenschutzbeauftragte vorgesehen.

5. Rollen und Verantwortlichkeiten

Verantwortlich für den Aufbau und die Aufrechterhaltung des Informationssicherheits- und Datenschutzmanagements ist der zentrale Informationssicherheitsbeauftragte (ZISB) des EGVs, der in seiner Tätigkeit durch ein Sicherheits-Team unterstützt wird. Der ZISB ist verantwortlich für die Erstellung und Inkraftsetzung sämtlicher, dieser Ordnung nachgelagerter, Richtlinien, Konzepte und Maßnahmen. Zudem wacht er über die Einhaltung der Vorgaben des Informationssicherheits- und Datenschutzmanagements. Der ZISB muss über die notwendige Fachkunde zur Erfüllung seiner Aufgaben verfügen.

6. Dokumentations- und Organisations-Struktur

Die Dokumentation ist folgendermaßen strukturiert:

- Ordnung: das oberste Management-Dokument mit der Ausrichtung des Informationssicherheits- und Datenschutzmanagements, erstellt durch das Informationssicherheits- und Datenschutz-Team und freigegeben durch den Generalvikar und den Leiter der Hauptabteilung Verwaltung

- Richtlinie: verbindliche Regelungen zu Zielen und Umsetzung von Informations-Sicherheit für alle Anwender und Dienstleister des EGV; wird erstellt vom zentralen Informationssicherheitsbeauftragten und freigegeben durch den Direktor der Hauptabteilung Verwaltung

- (techn.) Richtlinien: bereichsspezifische Regelungen, erstellt durch das Informationssicherheits- und Datenschutz-Team in Kooperation mit den relevanten Abteilungen und inkraftgesetzt durch den Direktor der Hauptabteilung Verwaltung
- Sicherheitskonzepte: technische Umsetzungen und organisatorische Maßnahmen, erstellt durch die Fachbereiche, geprüft durch das Sicherheits-Team und freigegeben durch den ZISB

7. Schutzziele und Risikoabschätzung

Um potenzielle Schadensfälle mit erheblichen, finanziellen und image-schadenden Auswirkungen zu identifizieren und Gegenmaßnahmen zu etablieren, wurden die folgenden Schutzziele definiert und die jeweiligen Anforderungen in den Fachabteilungen eruiert (Schutzbedarfsfeststellung):

- *Verfügbarkeit:* Begrenzung möglicher Ausfallzeiten auf ein akzeptables Maß, ohne gravierenden Einfluss auf den Dienst- und Geschäftsbetrieb. Planung von Maßnahmen zur Fortführung des Dienst- und Geschäftsbetriebs in Krisenszenarien.

- *Vertraulichkeit*: Schutz sensibler Informationen vor unbefugtem Zugriff sowie Gewährleistung der Gesetzeskonformität. Besondere Berücksichtigung finden die personenbezogenen Daten von Personal und Kirchenmitgliedern.

- *Integrität:* Gewährleistung der Unverfälschtheit und Korrektheit von Daten. Maßnahmen zur Rekonstruierung verlorengegangener Daten.

- *Authentizität:* Überprüfbarkeit und Richtigkeit der Identität des Urhebers einer Information. Nachvollziehbarkeit und Belegbarkeit von Handlungen.

Damit ein wirtschaftliches Verhältnis der Sicherheitsmaßnahmen zu den zu schützenden Werten gewährleistet werden kann, wurde eine Klassifikation in Schutzbedarfskategorien vorgenommen:

Verfügbarkeit:	
Wie lange können Sie auf ihre Anwendungen und Daten verzichten? Die Anforderung ist:	
Niedrig	Wenn die Daten nicht mehr verfügbar sind, entsteht ein nennenswerter Schaden nach 2 Wochen oder mehr.

Mittel	Wenn die Daten nicht mehr verfügbar sind, entsteht ein nennenswerter Schaden nach einer Woche.
Hoch	Wenn die Daten nicht mehr verfügbar sind, entsteht ein nennenswerter Schaden nach einem Tag.
Sehr hoch	Wenn die Daten nicht mehr verfügbar sind, entsteht ein nennenswerter Schaden nach 4 Stunden.

Vertraulichkeit:	
Wer darf Zugriff auf die Anwendungen und Informationen haben? Die Anforderung ist:	
Niedrig / Öffentlich	Wenn die Daten von der verantwortlichen Stelle für die Öffentlichkeit freigegeben wurden und keine weiteren Schutzmaßnahmen erforderlich sind (z.B. Pressemitteilung).
Mittel / Intern	Wenn die Daten für den internen Gebrauch bestimmt sind und ihre unkontrollierte Weitergabe nur sehr begrenzten Schaden verursachen kann. Schutzmaßnahmen müssen sicherstellen, dass Daten nicht unkontrolliert veröffentlicht werden.
Hoch / Vertraulich	Wenn der Zugriff auf bestimmte Gruppen eingeschränkt werden muss. Eine Veröffentlichung würde nur zu geringfügigen Schäden für das Erzbistum führen, wie z.B. bei Informationen über einen Teil des Geschäftes (z.B. Handbücher, Buchhaltungsdaten) oder bei Projektdokumenten.
Sehr hoch / Streng vertraulich	Wenn der Zugriff auf die Daten nur wenigen Personen erlaubt ist und die unkontrollierte Weitergabe der Daten sehr hohen Schaden anrichten kann,wie z.B. bei Daten aus der Seelsorgetätigkeit oder bei personenbezogenen Daten.

Integrität:	
Wie gravierend ist die unbefugte Verfälschung von Daten und wie leicht kann man sie erkennen? Die Anforderung ist:	
Niedrig	Wenn verlorengegangene oder abhanden gekommene Daten ohne Aufwand rekonstruiert werden können, eine Verfälschung direkt identifizierbar ist und keine Auswirkungen hat.
Mittel	Wenn verlorengegangene oder abhanden gekommene Daten ohne großen Aufwand rekonstruiert werden können, eine Verfälschung leicht identifizierbar ist und keine Auswirkungen hat.
Hoch	Wenn verlorengegangene oder abhanden gekommene Daten nur mit großem Aufwand rekonstruiert werden können, eine Verfälschung schwer identifizierbar ist und Auswirkungen hat.
Sehr hoch	Wenn verlorengegangene oder abhanden gekommene Daten auch mit großem Aufwand nicht rekonstruiert werden können, eine Verfälschung nicht identifizierbar ist und erhebliche Auswirkungen hat.

Authentizität:

Wie wichtig ist die Echtheit (Korrektheit) der Identität des Urhebers (Absenders) der Information? Die Anforderung ist:	
Niedrig	Wenn die Echtheit (Identität des Absenders) der Daten/Informationen nicht von Bedeutung ist.
Mittel	Wenn die Echtheit (Identität des Absenders) der Daten/Information von geringer Bedeutung ist.
Hoch	Wenn die Echtheit (Identität des Absenders) der Daten/Information von großer Bedeutung ist (Informationen aufgrund derer relevante Entscheidungen getroffen werden).
Sehr hoch	Wenn die Echtheit (Identität des Absenders) der Daten/Information von sehr großer Bedeutung ist (Informationen aufgrund derer sehr wichtige Entscheidungen mit ggf. rechtlichen Konsequenzen getroffen werden).

Die möglichen Auswirkungen denkbarer Bedrohungsszenarien werden in Form einer Auswirkungs- und Wahrscheinlichkeits-Analyse bewertet und eine Risikoklassifizierung gemäß Schadensstufe und Eintrittswahrscheinlichkeit der einzelnen Bedrohungen vorgenommen werden.

8. Fortschreibung und Review

Das aufgebaute Informationssicherheits- und Datenschutzmanagement soll fortlaufend in Verantwortung des zentralen Informationssicherheitsbeauftragten weiterentwickelt werden, um einerseits externe Änderungen umzusetzen, wie z.B. Gesetzesänderungen, andererseits aber auch neuen internen Herausforderungen gerecht zu werden. Diese Herausforderungen ergeben sich aus grundsätzlich neuen Anforderungen des Dienstgeschäftes, aus den Resultaten einer jährlichen Schutzbedarfs- und Risikoanalyse, können aber auch durch Eingaben und Hinweise von Mitarbeitenden eingebracht werden.

Die jährliche interne Schutzbedarfsfeststellung und eine externe Risikoanalyse in Form eines Audits dienen dazu, Veränderungen hinsichtlich schutzbedürftiger organisationseigener Werte sowie in der Einstufung des jeweiligen Schutzbedarfs zu überwachen.

Insgesamt folgt die Weiterentwicklung des Informationssicherheits- und Datenschutzmanagement dem PDCA-Prozessmodell [1], um kontinuierliche Anpassung und fortlaufende Aktualisierung zu gewährleisten. Ordnung, Sicherheitsrichtlinien und -konzepte sind Gegenstand jährlicher Reviews und können fallbezogen angepasst werden.

[1] Plan-Do-Check-Act-Lebenszyklus – Bestandteil der ISO27001: **P**lan – *planen*; **D**o – *testen, optimieren*; **C**heck – *auswerten, freigeben*; **A**ct - *umsetzen*

Diözesanadministrator

Köln; Datum: 14.5.14

Direktor HA-Verwaltung

Köln; Datum: 14.05.14