**Datenschutzprüfungen durch Gemeindeaufsichtsstellen (Musterbeispiel für einen Prüfungsbericht)**

**Datenschutzaufsichtsstelle der Gemeinde ...**

**Datenschutz und Informatiksicherheitsüberprüfung der Anwendung GeSoV (Geschäftskontrollsystem des Sozialdienstes und der Vormundschaftsabteilung)**

1. **Zusammenfassung**

Die Gemeindetreuhand AG ist für 4 Jahre gewählte Datenschutzaufsichtsstelle der Gemeinde. Gestützt auf die Kontrollvorgaben des Datenschutzgesetzes hat sie die Informatiksicherheit und den Datenschutz der Anwendung GeSoV geprüft. Die Prüfung umfasste die Rechtsgrundlagen für die Datenbearbeitung und die Zugriffsberechtigungen.

Massgebend für die Auswahl der Anwendung GeSoV als Prüfungsobjekt war, dass es sich um ein von der Gemeinde erst in den letzten Jahren eingeführtes System handelt. Die darin bearbeiteten Daten sind besonders schützenswert (Sozialhilfedaten, Vormundschaftsdaten). Die Gemeinde ist Sitzgemeinde des regionalen Sozialdienstes. Dies führt zu erheblichen Datenmengen.

GeSoV wird vom Sozialdienst und der Vormundschaftsverwaltung eingesetzt um praktisch alle Geschäfte zu behandeln. Die Datenspeicherung erfolgt in einer eigenen Datenbank. In GeSoV sind Daten enthalten, die sowohl der Vormundschaftsverwaltung als auch dem Sozialdienst zugänglich sind (Adressdaten). Daneben werden Daten bearbeitet, die den beiden angeschlossenen Abteilungen je getrennt zur Verfügung stehen sollen. Wird ein Worddokument erstellt, wird dieses mit dem im Geschäftskontrollsystem erfassten Geschäft verbunden. Die Ablage erfolgt dann auf dem ausserhalb der Datenbank gelegenen Datenserver. Die Anwendung stammt von einem externen Anbieter. Sie wird von der Gemeinde betrieben (Informatikdienst). Die Prüfung der Datenschutzaufsichtsstelle umfasste die beiden Bereiche

* Informatiksicherheit
* Datenschutz (ohne Informatiksicherheit)

Ein Schwergewicht der Prüfung galt der Ausgestaltung der Zugriffsrechte. Diese müssen sowohl aus einer rechtlichen wie auch aus einer informatiktechnischen Sicht korrekt ausgestaltet sein. Neben einer Prüfung, ob die Zugriffsberechtigungen den rechtlichen Grundlagen genügen, war zu prüfen, wie die rechtlichen Vorgaben organisatorisch und technisch umgesetzt sind.

Der Prüfbericht stützt sich auf eine Durchsicht der uns vorgelegten Dokumente des Sozialdienstes und der Vormundschaftsverwaltung. Zudem erfolgten Befragungen der Verantwortlichen in den beiden Abteilungen.

Die Datenschutzaufsichtsstelle kommt zum Schluss, dass die Vorgaben des Datenschutzrechtes durch GeSoV nicht vollumfänglich erfüllt werden. Verbesserungsbedarf sehen wir bei der Vergabe der Zugriffsrechte. Hier besteht ein kurzpflichtiger Handlungsbedarf. Es ist unzulässig, dass in GeSoV dem Leiter der Vormundschaftsverwaltung umfassend Zugriff auf Daten des Sozialdienstes und dem Leiter des Sozialdienstes umfassend Zugriff auf Daten der Vormundschaftsverwaltung gegeben wird.

Die Gemeinde benützt zum Bestimmen der Grundschutzmassnahmen die sogenannte Checkliste Grundschutz. GeSoV erfüllt mehrere dieser Vorgaben nicht oder nur teilweise. Hier sind Anpassungen vorzunehmen.

1. **Ergebnisse im Detail**

***B.a) Gegenstand der Überprüfung (Ziele)***

**B.a.a) Datenschutz (ohne Informatiksicherheit)**

* + Prüfung der Rechtsgrundlage für die Datenbearbeitung insgesamt und insbesondere die Rechtsgrundlagen für Abrufverfahren
  + Prüfung ob die Zugriffsrechte rechtmässig, insbesondere verhältnismässig, umschrieben und richtig umgesetzt sind
  + Prüfung der Umsetzung des Sperrrechts, des Berichtigungsanspruchs, der Datenvernichtung und der Archivierung sowie des Einsichtsrechts.

**B.a.b) Informatiksicherheit**

* Prüfung ob die durch die Gemeinde gemachten Vorgaben (Checkliste Grundschutz) sowie allfällige zum Zeitpunkt der Prüfung neu vorgegebenen Informatiksicherheitsmassnahmen umgesetzt sind (soweit dies für den Prüfungsgegenstand von Bedeutung ist)
* Prüfung ob die in Rechtssätzen, vor allem in Verordnungsbestimmungen (Datenschutzverordnung Art. 4-6) vorgegebenen Massnahmen für die Informatiksicherheit umgesetzt sind
* Vorschlag von zur Kontrolle zu verwendenden allfälligen Sollvorgaben, sofern für die Anwendung keine gemeindeeigenen Sollvorgaben bestehen, die den Stand der Technik genügend berücksichtigen.
* Überprüfung ob die aktuellen Grundschutzmassnahmen gemäss Grundschutzcheckliste für den Einsatz der Anwendung ausreichend sind
* Verifikation ob der Grundschutz nach Checkliste erfüllt, und evtl. pendente Massnahmen mit der Betriebsaufnahme umgesetzt sind.
* Überprüfung ob die, in der Risikobeurteilung erhöhten Schutzanforderungen durch geeignete Massnahmen abgedeckt sind.

Hauptsicht bei der Prüfung war das Umsetzen der Zugriffsrechte in GeSoV.

**B.a.c) Durchführung**

Die Prüfungen wurden durch Frau ....... und Herrn..... in der .... durchgeführt.

Bevor wir mit der Prüfung begonnen hatten, erstellten wir einen Prüfplan. Prüfungsumfang, anwendbare Regelungen, Weisungen und Vorgaben und die einzelnen Prüfungsschritte waren darin umschrieben.

**B.a.d) Termine**

|  |  |
| --- | --- |
| Erste Besprechung | ... |
| Prüfvorgang fertig gestellt | ... |
| Prüfungen durchführen | ... |
| Prüfungsbericht als Entwurf fertig gestellt | ... |
| Besprechung des Entwurfs mit den Vertretern des Sozialdienstes und der Vormundschaftsabteilung | ... |
| Abschluss des Prüfungsberichts und Abgabe an die beiden Abteilungen | ... |

**B.a.e) Befragungen**

Wir haben folgende Personen befragt:

- ..., Leiterin Sozialdienst

- ..., Leiter Vormundschaftsabteilung

- ..., Informatikadministrator der Gemeinde

- ... (Benutzer beim Sozialdienst)

- ... (Benutzerin bei der Vormundschaftsverwaltung)

**B.a.f) Beigezogene Unterlagen**

Die beiden Abteilungen stellten uns folgende Dokumente zur Verfügung:

* Benutzerdokumentation GeSoV

- GeSoV Arbeitsplatzeinstellungen

* GeSoV Umgang mit Geschäften
* GeSoV Adressdaten
* Grobübersicht GeSoV
* Vorgehen bei Systemausfall von GeSoV
* Datensicherungsvorgaben GeSoV
* ....
* ....
* Einsatz von Druckern in GeSoV

Hinzu kamen eine Dokumentation, wie generell Benutzerrechte erteilt werden sowie die uns teilweise vorgängig zugestellten, teilweise erst von uns anlässlich der Besichtigungen verlangten Bildschirmausdrucke.

Insbesondere als Soll-Vorgabe für die Informatiksicherheit verwendeten wir neben der bereits erwähnten Checkliste Grundschutz die auf der Intranetseite des Kantons Bern publizierten, derzeit gültigen Informatiksicherheitsvorgaben. Diese wurden uns freundlicherweise vom IT-SIBE (Informationstechnologie-Sicherheitsbeauftragter des Kantons Bern) vom kantonalen Amt für Informatik und Organisation (KAIO) zur Verfügung gestellt. Die übergeordneten rechtlichen Grundlagen finden sich im Sozialhilfegesetz, im Einführungsgesetz zum Schweizerischen Zivilgesetzbuch und im Schweizerischen Zivilgesetzbuch, im Gesetz über die Verwaltungsrechtspflege sowie im kantonalen Datenschutzgesetz (KDSG).

**B.a.g) In der Anwendung GeSoV untersuchte Teilsysteme**

- Benutzer- und Zugriffsberechtigungsverwaltung (Stichproben)

- GeSoV-Datenbankserver (die Sicherheitskonfigurationseinstellungen wurden einzig stichprobenweise geprüft)

- Citrix-Server (die Sicherheitskonfigurationseinstellungen des Windows-Betriebssystems wurden einzig stichprobeweise geprüft)

- Zu den überprüften Systemen ist auf Folgendes hinzuweisen:

Anwendung GeSoV: Alle Daten werden im GeSoV zentral gespeichert. Das ermöglicht einen gemeinsamen Zugriff auf sämtliche Geschäfte einer Abteilung. Der Informatikbeauftragte der Gemeinde übernimmt die Datensicherung.

- In GeSoV besteht eine eigene Passwort- und Benutzerverwaltung

Auf die Daten wird über den GeSoV-Client zugegriffen. Dieser läuft auf dem Citrix-Server. Die Anwendung GeSoV speichert die Daten in einer eigenen Datenbank ab. Word- und Excel-Dateien sind auf dem üblichen Laufwerk B für Office-Anwendungen gespeichert. Um auf die Datenbank zuzugreifen besteht ein so genannter technischer Benutzer. Damit ist es unnötig, dass GeSoV-Benutzende eigene Benutzerkonten auf der Datenbank haben.

- Citrix-Metaframeserver und Datenbankserver von GeSoV

Beide Server werden im Betriebssystem Windows betrieben. Der Informatikverantwortliche der Gemeinde ist für deren Betrieb und Unterhalt verantwortlich.

- Datenbank GeSoV

Ein Ausfall dieser Datenbank führt zu einem Totalausfall des gesamten Systems. Eine redundante Datenbank fehlt. Der bei einem Ausfall die Datenbank entstehende Arbeitsunterbruch von bis zu 2 Tagen wird von beiden Abteilungen als tragbar beurteilt.

***B.b) Handlungsbedarf***

Aus der unten stehenden Tabelle wird ein zusammenfassender Überblick unserer Hinweise und unserer Einschätzung des Handlungsbedarfs (sofort, innert Jahresfrist, später) ersichtlich. In den nachfolgenden Kapiteln erfolgen detaillierte Erläuterungen zu den Feststellungen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Gegenstand** | **sofort** | **innert Jahresfrist** | **später** |
| Datenschutz (ohne Informatiksicherheit) | | | |
| a) Die Abteilungsleiter haben auf GeSoV-  Daten beider Abteilungen Zugriff | X |  |  |
| b) Anmeldung im Register der Datensamm-  lungen |  | X |  |
| c) Löschungs- und Archivierungskonzept   fehlt |  | X |  |
| Informatiksicherheit | | | |
| a) Das Personal wird zur Informatiksicherheit der Anwendung nicht ausgebildet |  | X |  |
| b) Restore-Prozess aktuell nicht geprüft ^.^^„ Restor^Prozess | X |  |  |
| c) Aufbewahrung der Backups ausserhalb des Betriebes | X |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

***B.c) Datenschutz***

**B.c.a) Anwendbarkeit des Kantonalen Datenschutzgesetzes (KDSG)**

Die beiden Abteilungen Sozialdienst und Vormundschaftsverwaltung benutzen GeSoV bei der Abwicklung praktisch aller Geschäfte. Das KDSG ist nur anwendbar, soweit es nicht um hängige Justizverfahren geht. Solche werden im GeSoV nicht abgewickelt. Die regelmässig abgewickelten erstinstanzlichen Verwaltungsverfahren unterstehen dem kantonalen Datenschutzgesetz. Schliesslich findet GeSoV auch Anwendung, wenn Verfahren abgeschlossen sind.

**B.c.b) Bestehen genügende Rechtsgrundlagen für die Datenbearbeitung**

Das Bearbeiten von Daten ist zulässig, wenn das Gesetz ausdrücklich dazu ermächtigt. Werden – wie in GeSoV – besonders schützenswerten Daten bearbeitet, so muss sich die Zulässigkeit aus einer gesetzlichen Grundlage klar ergeben. Sowohl die Sozialhilfegesetzgebung als auch die Einführungsgesetzgebung zum Zivilgesetzbuch und das Zivilgesetzbuch verpflichten die Gemeinde die Sozialhilfeaufgaben und die Vormundschaftsaufgaben wahrzunehmen. Die Verwaltung der in beiden Bereichen anfallenden Geschäfte in einer elektronischen Geschäftskontrolle ist zur Aufgabenerfüllung unabdingbar. Die für die beiden Aufgabenbereiche bestehenden Rechtsgrundlagen erlauben die Datenbearbeitung damit.

**B.c.c) Genügende Rechtsgrundlage für ein Abrufverfahren?**

Beide Abteilungen haben einen Zugriff auf das Einwohnerkontrollsystem EWK2000. Eine Schnittstelle zu GeSoV fehlt aber. Der Zugriff auf EWK2000 bildet damit nicht Gegenstand der Prüfung. Durch die bestehende Möglichkeit, dass der Leiter der einen Abteilung auf Daten der anderen Abteilung zugreifen kann, liegt ein Abrufverfahren vor (Zugriff einer andern Organisationseinheit im Selbstbedienungsverfahren auf Daten die bei einer anderen Organisationseinheit zu einem andern Zweck bearbeitet werden). Ein solcher Zugriff - hier auf besonders schützenswerte Daten - bedingt eine Rechtsgrundlage in einem vom Souverän der Gemeinde beschlossenen Reglement. Eine solche Rechtsgrundlage fehlt. Da es sich aber in unserer Prüfung gezeigt hat, dass das Abrufverfahren durch ein Aufheben der Zugriffsrechte der Abteilungsleiter abzuschaffen ist, ist auf die fehlende Rechtsgrundlage für ein Abrufverfahren nicht weiter einzugehen.

**B.c.d) Umfang der Zugriffsrechte**

Für GeSoV wird allen Mitarbeitenden je ein eigenes Benutzerkonto zur Verfügung gestellt. Zur Verfügung stehen sämtliche Daten ab Inbetriebnahme von GeSoV (2005). In der Vormundschaftsverwaltung haben 3 Mitarbeitende Zugriff, im Sozialdienst 5. In beiden Abteilungen ist es so, dass die Mitarbeitenden entweder Aufgaben zu allen Klienten haben (Sekretariate) oder diese Aufgaben zumindest im Stellvertretungsfall bestehen. Es zeigt sich damit, dass die zum Zugriff offenen Daten für die jeweilige Aufgabenerfüllung der Mitarbeitenden erforderlich sind. Insbesondere ist es nicht so, dass die Klienten auf die Sachbearbeitenden nach bestimmten Kriterien (Alphabet, Wohnort etc. zugeteilt werden). Die Zuteilung erfolgt vielmehr in Abhängigkeit des Eingangszeitpunkts eines Geschäftes oder der Arbeitslast.

Die beiden für die Abteilungsleitung verantwortlichen Personen haben je auf den gesamten Datenbestand von GeSoV Zugriff. Dieser Zugriff wurde bei Einführung des Systems 2005 so festgelegt. Eine nähere Begründung für dieses Vorgehen konnte den Prüfenden nicht gegeben werden. Dagegen steht fest (und wurde von beiden abteilungsleitenden Personen auch nicht in Abrede gestellt), dass es beiden an Aufgaben in der andern Abteilung je fehlt. Die Stellvertretungsfunktionen sind abteilungsintern zugewiesen und es ist gerade nicht Sache der Abteilungsleiter, sich gegenseitig zu vertreten. Der je GeSoV-weit gegebene Zugriff ist damit rasch durch je einen abteilungsweiten Zugriff zu ersetzen.

**B.c.e) Recht auf Sperrung**

Sozialhilfedaten und regelmässig auch die von der Vormundschaftsabteilung bearbeiteten Daten sind besonders schützenswert. Die Bekanntgabe solcher Daten an Private ist auch im Rahmen der Informationsgesetzgebung unzulässig. Es fehlt damit in der Hauptsache an einem Bedürfnis, Datensperren zu verlangen. Nicht auszuschliessen ist jedoch, dass vereinzelt Private gestützt auf die Informationsgesetzgebung Angaben über Personen oder Personengruppen verlangen könnten (z.B. Liste aller Beistände, die Gemeinde hat im Organisationsreglement eine Rechtsgrundlage für Listenauskünfte geschaffen). GeSoV kennt zur Umsetzung dieses Sperrechtes ein Datenfeld (Sperrcode).

**B.c.f) Einsichtsrecht**

GeSoV erlaubt den Ausdruck aller Daten in einer Weise, die es gestattet, einer interessierten Person die Ausübung ihres Einsichtsrechts zu ermöglichen. Insbesondere ist es nicht erforderlich, manuell allenfalls nicht zugängliche Daten (überwiegende Drittinteressen etc.) abzudecken. Ein den Umfang des Einsichtsrechts berücksichtigender Ausdruck lässt sich vielmehr elektronisch erstellen. Das System erlaubt damit die Umsetzung des Einsichtsrechts.

**B.c.g) Berichtigungsrecht**

Art. 23 KDSG gibt den Betroffenen einen Anspruch darauf, dass unrichtige oder nicht notwendige Personendaten über sie berichtigt oder vernichtet werden. Das System lässt Korrekturmöglichkeiten zu, die dem Berichtigungsanspruch genügen. Ebenfalls technisch umsetzbar ist die in Art. 23 Abs. 3 KDSG vorgesehene Gegendarstellung.

**B.c.h) Löschung / Datenvernichtung**

Art. 19 Abs. 1 KDSG verlangt, dass nicht mehr benötigte Daten zu vernichten sind. Vorbehalten bleibt die Einlieferung in das Gemeindearchiv. Der Weisung des Amtes für Gemeinden und Raumordnung „Gemeindearchive/Aktenaufbewahrung in den Gemeinden“ vom 24.9.2007 (BSIG Nr. 1/170.111/3.1) ist unter Ziff. 6 zu entnehmen, dass Sozialhilfeakten 15 Jahre nach Einstellung des Sozialhilfeleistung bzw. 10 Jahre nach einem Todesfall zu vernichten sind. Ziff. 4 der Weisung gibt für Vormundschaftsdaten in der Regel 30-jährige Aufbewahrungsfristen vor. In GeSoV besteht einzig eine Möglichkeit zur Dokumentenlöschung. Es ist sicherzustellen, dass der Anbieter eine Lösung zur Verfügung stellt, die es auch erlaubt, eigentliche GeSoV-Einträge (elektronische Karteien der Geschäftskontrolle) ausserhalb von Office-Dokumenten zu löschen. Als zweites muss ein Löschungs- und Archivierungskonzept erstellt werden. Dieses hat sicherzustellen, dass das System beim Fallabschluss (im Sozialhilfebereich Einstellung der Unterstützung) die in der AGR-Weisung vorgegebenen Löschfristen umsetzbar macht. Es muss möglich sein, mittels eines Suchlaufes zu einem bestimmten Zeitpunkt diejenigen Geschäfte festzustellen, die zu löschen oder ins Archiv überzuführen sind. Schliesslich ist dafür zu sorgen, dass für diejenigen Geschäfte, die in GeSoV nach Abschluss zu Beweiszwecken aufbewahrt werden (Kategorie B im Sinne der Weisung des AGR) nur ein erheblich eingeschränkter Personenkreis Zugriff hat. Nach den Darstellungen der beiden Abteilungsleitenden wird ein Fall ausnahmslos nur durch das Sekretariat wiedereröffnet. Gleiches gilt für die seltenen aus andern Gründen bei abgeschlossenen Fällen erforderlichen Nachprüfungen. Es ist daher unverhältnismässig, wenn den nur mit aktuell hängigen Fällen befassten Mitarbeitenden ein umfassender Zugriff auch auf alle abgeschlossenen Fälle gegeben wird.

**B.c.i) Feststellungen und Empfehlungen im Bereich Datenschutz (mit detaillierteren Angaben)**

*(Dieser Abschnitt ist nur erforderlich, wenn aus den vorangehenden Darstellungen insbesondere zu wenig klar ist, was die geprüfte Stelle vorzukehren hat Hier wird darauf verzichtet.)*

***B.d)******Informatiksicherheit***

**B.d.a) Vorgaben und Weisungen**

Die Gemeinde (Gemeinderatsbeschluss vom... ) stellt auf die Checkliste Grundschutz ab.

**B.d.b) Durcharbeiten der Checkliste Grundschutz** *(Es wird nur ein kleiner Auszug aus der Checkliste Grundschutz dargestellt. In einer umfassenden Prüfung der Informatiksicherheit müsste die ganze Liste abgearbeitet werden)*

Auszug aus der Checkliste Grundschutz

**B.d.c) Hinweise und Empfehlungen im Bereich Informatiksicherheit detailliert**

Beispiel-Massnahmenliste ISDS Grundschutz

**C)** **Abschliessender Hinweis**

Unsere Feststellungen stützen sich auf die uns zugestellten Informationen und Dokumentationen sowie auf unsere Erhebungen und auf die durchgeführten technischen Prüfungen. Bei allen kontaktieren Mitarbeitenden der beiden Abteilungen bedanken wir uns für die gewährte Unterstützung.

Ort, Datum: Unterschrift:

.................................................................. ..........................................................