Kanton Bern
Canton de Berne

Datenschutzaufsichtsstelle (DSA)

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
datenschutz@be.ch
www.dsa.be.ch

Datenschutz: Periodische Prüfungen der Informatikanwendungen: RAHMENBEDINGUNGEN

(auch für den Beizug externer Kontrollstellen)

Inhaltsverzeichnis

Wer eine unabhängige externe Fachstelle mit einer Datenschutzkontrolle beauftragen will oder Datenschutzaufsichtsstellen, die eine Datenschutzkontrolle in eigener Regie durchzuführen beabsichtigen, haben folgende Rahmenbedingungen einzuhalten:

1. Erteilung des Kontrollmandates bei Beizug einer externen Fachstelle[1]

Es ist ein schriftlicher Vertrag basierend auf den Allgemeinen Geschäftsbedingungen (AGB) der Schweizerischen Informatikkonferenz (SIK[2]), abzuschliessen.

2. Inhalt der Kontrolle

2.1 Grundsatz: Anwendungskontrolle

- Zu prüfen ist anwendungsbezogen die Einhaltung der rechtlichen Vorgaben (behördliche Kontrolle, kein Datenschutzaudit keine Zertifizierung).
- Lassen die anwendbaren Normen Beurteilungs- oder Ermessensspielräume, soll einzig die Vertretbarkeit der getroffenen Lösung geprüft werden.

2.2 Gegenstand der Kontrolle

Folgendes ist kombiniert oder einzeln zu prüfen:

2.2.1 Datenschutz (ohne Informatiksicherheit)

Die Prüfstelle nimmt bei dieser Prüfung folgende Prüfungshandlungen vor:

- Sie prüft die Rechtsgrundlagen für die Datenbearbeitung insgesamt und insbesondere die Rechtsgrundlagen für Abrufverfahren.
- Sie prüft, ob die Zugriffsrechte rechtmässig, insbesondere verhältnismässig umschrieben und richtig implementiert sind.
    - Soweit die präventiven Massnahmen den verhältnismässigen Zugriff nicht sicherstellen,
    - prüft die Prüfstelle, ob die rechtmässige Ausübung der Zugriffsrechte durch Kontrollmassnahmen wie Protokollierung sichergestellt ist (Art. 6 DSV[3]), wie diese implementiert sind und wie sie eingesetzt werden.
- Sie prüft, ob und wie
    - das Sperrrecht,
    - der Berichtigungsanspruch,
    - die Datenvernichtung und die Archivierung sowie
    - das Einsichtsrecht

  umgesetzt sind.

[1] Der Beizug externer Kontrollstellen wurde für die Kantonsverwaltung ab 2004 als Arbeitsmittel eingesetzt; erstmals umschrieben in RRB 1668/04 vom 26. Mai 2004.
[2] http://www.sik.admin.ch/
[3] Datenschutzverordnung vom 22. Oktober 2008; DSV; BSG 152.040.1

2.2.2 Informatiksicherheit

Die Prüfstelle nimmt bei der Prüfung der Informatiksicherheit folgende Prüfungshandlungen vor:

- Sie prüft, ob die vom Gemeinderat und allfällige zum Zeitpunkt der Prüfung neu vorgegebene Informatiksicherheitsmassnahmen umgesetzt sind.
- Sie prüft, ob die in Rechtssätzen, insbesondere die in den Art. 4 - 5 DSV gemachten Vorgaben für die Informatiksicherheit umgesetzt sind.
- Sie macht Vorschläge, welche Sollvorgaben sie zur Kontrolle verwenden will, wenn für die Anwendung keine gemeindeeigenen, den Stand der Technik genügend berücksichtigenden Sollvorgaben bestehen und prüft deren Umsetzung.

2.2.3 Datenschutzorganisation

- Die Prüfstelle prüft, ob die Verantwortlichkeiten im Sinne von Art 8 KDSG[4] klar sind und prüft summarisch, ob und wie die Verantwortlichen ihre Führungsaufgaben wahrnehmen.

3. Anforderungen an unabhängige externe Fachstellen

3.1 Fachliche Anforderungen

Die Fachstelle muss über informatiktechnisches Fachwissen, über rechtliches Wissen und über Wissen, wie Kontrollhandlungen durchzuführen sind (Revisionswissen) verfügen. Nachzuweisen ist dies dadurch, dass die Fachstelle aufzeigt, dass ihr Personen mit einem juristischen Hochschulabschluss, Personen mit einer Fachhochschulausbildung in Informatik oder einer dieser Ausbildung entsprechenden Ausbildung oder einer längeren Berufspraxis in diesem Umfeld und Personen mit einer Informatik-Auditoren-Ausbildung oder einer längeren Berufspraxis in diesem Umfeld zur Verfügung stehen.

3.2 Unabhängigkeit

- Die externe Fachstelle muss unabhängig sein.
- Das heisst insbesondere, dass als unabhängige Fachstelle nicht eingesetzt werden dürfen:
    - Ehemalige Mitarbeitende, die für die Informatikanwendung verantwortlich waren,
    - In die Projektleitung einbezogene Stellen,
    - Stellen, die Teilaufträge zum Betrieb der Informatikanwendung übernahmen, Outsourcingpartner für die Anwendung.

4. Unterstellung unter das Amtsgeheimnis

- Soweit es um Personendaten geht, wird die externe Fachstelle durch Art. 2 Abs. 5 Buchst. b KDSG zur Behörde. Sie untersteht damit dem Amtsgeheimnis. Für die übrigen Daten erfüllen die unabhängigen externen Fachstellen gestützt auf Art. 64 GG[5] einen amtlichen Auftrag und unterstehen damit ebenfalls dem Amtsgeheimnis.

[4] Datenschutzgesetz vom 19. Februar 1986: KDSG; BSG 152.04
[5] Gemeindegesetz vom 16. März 1998; GG; BSG 170.01

- Die das Kontrollmandat erteilende Stelle weist die unabhängige externe Fachstelle im schriftlichen Vertrag auf die Unterstellung unter das Amtsgeheimnis und auf die Straffolgen hin. Sie verpflichtet in diesem Vertrag die unabhängige externe Fachstelle alle an Kontrollhandlungen beteiligten Personen eine Geheimhaltungserklärung, die das Amtsgeheimnis und die Straffolgen erwähnt, unterzeichnen zu lassen.

5. Pflicht ein Prüfungsprogramm zu erstellen

Bevor die unabhängige externe Fachstelle mit den eigentlichen Prüfungshandlungen beginnt, hat sie der verantwortlichen Stelle einen Prüfplan auszuhändigen, der darlegt

- Ziel und Umfang der Kontrolle
- Den Zeitabschnitt, worin die zu kontrollierenden Datenbearbeitungen stattgefunden haben dürfen (z. B. auch archivierte Daten, etc.)
- Die zu berücksichtigenden Vorschriften des Datenschutzgesetzes
- Die zu berücksichtigenden weiteren Vorschriften und Weisungen
- Die Klassifizierung der Daten
- Die zu berücksichtigenden Informatiksicherheitssollvorgaben
- Die vorgesehenen Kontrollmittel gemäss Ziffer 6, insbesondere das Konzept für Stichproben sowie deren Anzahl, Inhalt und Prüfungsziel
- Den erforderlichen Zugriff auf Informatikmittel
- Den geschätzten Zeitbedarf der Kontrolle
- Die für die Kontrollhandlungen vorgesehenen Personen
- Die Termine für die Kontrollhandlungen und den Endtermin für die Ablieferung des Kontrollberichts.

6. Kontrollmittel

Die unabhängige externe Fachstelle soll als Kontrollmittel mündliche oder schriftliche Befragungen von Mitarbeitenden, Unterlagen, Vorführungen von Informatikanwendungen, Zugriffe auf Informatikmittel, Dateien, insbesondere Protokolldateien, sowie technische Messungen und Tests auch im Sinne des „ethical hackings" einsetzen. In der Regel hat sie sich bei der Prüfung der Datenlage auf Stichproben zu beschränken.

7. Ergebnis

Die unabhängige externe Fachstelle hat einen Kontrollbericht abzufassen. Darin soll detailliert dargelegt sein, welche Ergebnisse die im Prüfplan aufgezeigten Kontrollhandlungen gezeigt haben. Der Kontrollbericht soll sich über die Erfüllung und den Erfüllungsgrad der Sollvorgaben äussern. Er soll zudem eine Gesamtbeurteilung enthalten. Zeigt der Bericht Mängel auf, soll er Empfehlungen für Verbesserungsmassnahmen enthalten. Der Bericht ist der verantwortlichen Stelle an einer Sitzung zu erläutern.

0. ERLÄUTERUNGEN

1. Allgemeines

1.1 Ausgangslage

Das Dokument „RAHMENBEDINGUNGEN“ legt die generellen Rahmenbedingungen für die Durchführung einer Informatikanwendungskontrolle sowie für den allfälligen Beizug externer Datenschutzkontrollstellen fest.

1.2 Rechtliches zum Beizug externer Datenschutzkontrollstellen

Mit einem solchen Beizug geht es um die Auslagerung einer behördlichen Kontrolle an externe Stellen. Rechtsgrundlage für die Aufgabenauslagerung an externe Stellen bildet Art 64 Abs. 1 GG.

2. Erläuterungen zu den einzelnen Ziffern

2.1 Organisatorisches (Ziffer 1 der RAHMENBEDINGUNGEN)

Erfolgt der Beizug einer externen Kontrollstelle haben die Verträge mit dieser auf den Allgemeinen Geschäftsbedingungen (AGB) der Schweizerischen Informatikkonferenz (SIK) zu basieren.

2.2 Inhalt der Kontrolle (Ziffer 2 der RAHMENBEDINGUNGEN)

2.2.1 Anwendungskontrolle (Ziffer 2.1 der RAHMENBEDINGUNGEN)

Art. 43 USG[6] sieht für den Umweltschutzbereich vor, dass die Vollzugsbehörden Private mit Kontrollaufgaben betrauen können. Die aus diesem Umfeld bekannten Vorgehensweisen werden inzwischen von privaten Anbietern auch für Datenschutzkontrollen bei Behörden und Privaten angeboten. Im Zentrum der Kontrollhandlungen steht hierbei die Führung, das sogenannte Datenschutzmanagement. Die Detailkontrolle einer Informatikanwendung stellt nur einen kleinen Teilbereich der gesamten Kontrollhandlungen dar. Anbieter solcher Kontrollhandlungen, mit denen in der Regel die Erteilung eines Datenschutzzertifikates verbunden ist, können als externe unabhängige Kontrollstelle durchaus in Frage kommen. Es ist aber in aller Deutlichkeit zu sagen, dass ihr Auftrag sich auf eine behördliche Anwendungskontrolle beschränkt. Zertifizierungen sind im kantonalen Recht nur für Vorabkontrollen relevant. Das schliesst nicht aus, dass sich Amtsstellen für eine solche Zertifizierung interessieren. Wenn sie es tun, geschieht dies aber ausserhalb der mit den RAHMENBEDINGUNGEN gemachten Vorgaben. Die vollständige Übernahme eines im Hinblick auf eine Zertifizierung vorgegebenen Kontrollrahmens ist daher regelmässig nicht zielführend.

Nicht anders als bei Umweltschutzkontrollen wird die unabhängige externe Fachstelle sich Spielräumen gegenübersehen. Unbestimmte Rechtsbegriffe können Beurteilungsspielräume eröffnen oder Regelun-

[6] Bundesgesetz vom 7. Oktober 1983 über den Umweltschutz; USG; SR 814.01

gen können der für die Informatikanwendung verantwortlichen Stelle Ermessen einräumen. Die kontrollierende Stelle soll Beurteilungen und Ermessensausübungen immer dann übernehmen, wenn sie den von der Norm gesetzten Rahmen respektieren. Eine Kontrolle der Beurteilung oder Ermessensausübung soll nicht erfolgen[7].

2.2.2 Kontrolle des Datenschutzes ohne Kontrolle der Informatiksicherheit (Ziffer 2.2.1 der RAHMENBEDINGUNGEN)

Bei der hier umschriebenen eigentlichen Persönlichkeitsschutzkontrolle geht es darum, zu prüfen, ob die vom Datenschutzgesetz gegebenen Vorgaben eingehalten sind. Nicht zu prüfen ist das Einhalten der Vorgabe des Datenschutzgesetzes zur Informatiksicherheit (Art. 17 KDSG). Zu prüfen ist also, ob das Sperrecht im System umgesetzt ist, ein Berechtigungsanspruch umgesetzt werden kann, ob und wie die Daten archiviert und vernichtet werden und ob und wie das Einsichtsrecht umgesetzt werden kann. Die Kontrolle könnte etwa zeigen, dass ein Datenfeld zur Aufnahme einer Sperrung fehlt oder dass eine Datenvernichtung im System gar nicht möglich oder aber organisatorisch nicht vorgesehen ist.

Ein Schwergewicht wird bei der Prüfung der bestehenden Zugriffsrechte liegen. Es geht darum, zu klären, ob die an die Anwendung angeschlossenen Mitarbeitenden nur auf diejenigen Informationen Zugriff haben, die sie für ihre Aufgabe benötigen. Es kann sich zeigen, dass bereits die theoretische Umschreibung der Zugriffsrechte zu offen ist. Auch wenn diese korrekt vorgenommen worden ist, ist aber möglich, dass das System die vorgegebenen Grenzen tatsächlich nicht respektiert oder Umgehungen zulässt.

Eine schwergewichtig rechtliche Prüfung ist diejenige nach dem Vorhandensein der Rechtsgrundlagen, vor allem auch für Abrufverfahren (Zugriffe durch eine Drittstelle im Selbstbedienungsverfahren). Nachdem sich auch das für Vorabkontrollen verlangte ISDS-Konzept für Informatikprojekte an den Vorgaben des Datenschutzgesetzes orientieren muss, decken sich die Prüfpunkte im Wesentlichen mit den in einem ISDS-Konzept zu erläuternden Umsetzungen der Persönlichkeitsschutz-rechte.

Gerade im Bereich des Datenschutzes ohne Informatiksicherheit wurden bisher kaum Kontrollen durchgeführt. Diese gesetzwidrige Untererfüllung des Kontrollauftrages soll behoben werden.

2.2.3 Kontrollen der Informatiksicherheit (Ziffer 2.2.2 der RAHMENBEDINGUNGEN)

- Hier geht es darum, zu prüfen, ob die vom Gemeinderat gemachten Vorgaben eingehalten werden (Art. 17 KDSG).
- Vereinzelt machen spezifische Verordnungsbestimmungen zusätzliche Vorgaben zur Informatiksicherheit. Als Verordnungsbestimmungen jedenfalls zu berücksichtigen sind aber die Artikel 4 bis 5 DSV. Darin sind die Risiken, vor denen die Systeme zu schützen sind und die erforderlichen technischen und organisatorischen Massnahmen umschrieben.
- Nicht auszuschliessen ist, dass die bestehenden Sollvorgaben zur Informatiksicherheit keine Regelungen für die zu prüfende Informatikanwendung geben. In diesem Fall hat die Prüfstelle oder die mit der Prüfung beauftragte unabhängige externe Kontrollstelle festzulegen, welche Normen lückenfüllend übernommen und geprüft werden sollen. Zu denken ist beispielsweise an die Checkliste Minimale Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf des Bundes[8].

[7] Siehe auch Alexander Rossnagel, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden 2000.
[8] https://www.isb.admin.ch/isb/de/home/themen/sicherheit.html

2.2.4 Datenschutzorganisationen (Ziffer 2.2.3 der RAHMENBEDINGUNGEN)

Art. 8 KDSG definiert die für die Datenbearbeitung verantwortliche Behörde. Insbesondere verlangt diese Bestimmung, dass, wenn Datenbearbeitungen durch mehrere Behörden erfolgen, eine gesamtverantwortliche Behörde bezeichnet wird. Mit dieser Verantwortungszuweisung sind Führungsaufgaben verbunden. Die Prüfstelle wird im Rahmen ihrer anwendungsbezogenen Kontrollen feststellen, wie die verantwortliche Behörde ihre Führungsaufgabe wahrnimmt. Über solche Feststellungen soll sie summarisch berichten.

2.3 Anforderungen an die unabhängige externe Fachstelle (Ziffer 3 der RAHMENBEDINGUNGEN)

2.3.1 Fachwissen (Ziffer 3.1 der RAHMENBEDINGUNGEN)

- Bereits im Vortrag zum KDSG vor über 20 Jahren wurde festgehalten, eine Datenschutzkontrolle erfordere juristisches, informatiktechnisches und organisatorisches Wissen. Die Anforderungen an die Kontrolleure sind zum heutigen Zeitpunkt die gleichen.
- Zu präzisieren ist, dass das organisatorische Wissen mit Wissen über Kontrollen (Revisionswissen) verbunden sein muss.
- Ob dieses Wissen bei den sich für Kontrollhandlungen anbietenden Stellen vorhanden ist, ist unter Umständen schwierig zu prüfen. Nachzuweisen haben sie, dass sie Personen beiziehen können, die über entsprechende Ausbildungen oder über eine längere Berufserfahrung verfügen. Ob es sich bei diesen beizuziehenden Personen um Mitarbeiter oder um anderweitig eingebundene Personen handelt (Konsortien), ist unerheblich. Bei Teilprüfungen können Fachkenntnisse im entsprechenden Teilbereich (z.B. Informatiksicherheit) genügen. Ein Nachweis über genügendes Fachwissen kann auch dadurch erbracht werden, dass eine Ausbildung einer anerkannten Organisation durchlaufen worden ist (z.B. ISACA)[9].

2.3.2 Unabhängigkeit (Ziffer 3.2 der RAHMENBEDINGUNGEN)

Anstoss zur Einführung von Kontrollen ist die festgestellte chronische Untererfüllung des Kontrollauftrages im Datenschutz. Dem gesetzlichen Kontrollauftrag kann nur dann Genüge getan werden, wenn die Prüfstelle glaubhaft ist. Das setzt in erster Linie Unabhängigkeit voraus. Weder darf die Prüfstelle von ihr selbst zu verantwortende frühere Handlungen überprüfen, noch am Betrieb der aktuellen Informatikanwendung beteiligt sein.

Art. 9 VRPG[10] verfolgt für das Verwaltungsverfahren und das Verwaltungsjustizverfahren dieselben Ziele. Die Verfasser der RAHMENBEDINGUNGEN haben sich bei ihrer Vorgabe an dieser Bestimmung orientiert.

[9] Siehe zu dieser Vereinigung: http://www.isaca.ch/ insbesondere zum Fachausweis CISA
[10] Gesetz vom 23. Mai 1989 über die Verwaltungsrechtspflege; VRPG; BSG 155.21

2.4 Unterstellung externer Fachstellen unter das Amtsgeheimnis (Ziffer 4 der RAHMENBEDINGUNGEN)

Eine allenfalls beigezogene unabhängige externe Fachstelle übt Behördeaufgaben aus. Es muss jedenfalls sichergestellt sein, dass die Kontrollstelle nicht ihrerseits zu einer Gefahr für die Geheimhaltung wird. Art. 2 Abs. 5 KDSG und Art. 64 GG bilden die Rechtsgrundlage für eine Unterstellung der Kontrollstelle unter das Amtsgeheimnis. Sie untersteht damit der Strafdrohung von Art. 320 StGB[11]. Im Vertrag soll die unabhängige externe Fachstelle zur Geheimhaltung verpflichtet und an das Amtsgeheimnis erinnert werden. Sie hat zudem alle an Kontrollhandlungen beteiligte Mitarbeitende eine Geheimhaltungserklärung unterzeichnen zu lassen.

2.5 Pflicht ein Prüfungsprogramm zu erstellen (Ziffer 5 der RAHMENBEDINGUNGEN)

Die RAHMENBEDINGUNGEN machen hierzu detaillierte Vorgaben. Informatikanwendungen bearbeiten in der Regel grosse Datenmengen. Die möglichen Datenbearbeitungen sind zahlreich, die sich stellenden datenschutzrechtlichen Fragen nicht selten komplex. Wer eine Informatikanwendung datenschutzrechtlich überprüfen soll, läuft Gefahr, sich zu verlieren. Dieser Gefahr soll durch den Prüfplan begegnet werden. Die Prüfstelle soll darlegen, wie sie bei der Prüfung vorgehen will und wo sie ihre Prüfungshandlungen begrenzt. Es soll damit möglich sein, vor der Kontrolle zu beurteilen, ob ein sinnvolles Kontrollverfahren vorgesehen ist.

2.6 Kontrollmittel (Ziffer 6 der RAHMENBEDINGUNGEN)

Mit der Aufzählung der Kontrollmittel soll der Prüfstelle dargelegt werden, welche Mittel sie einsetzen kann und welche nicht. Neben den bei Revisionen gängigen Mitteln (Befragungen, Konsultation von Unterlagen) sollen auch Vorführungen von Informatikanwendungen, technische Messungen, Zugriffe auf Informatikmittel und Dateien sowie allenfalls ein «ethical hacking» zulässig sein (Versuch in ein Informatiksystem einzudringen um den für das System Verantwortlichen Sicherheitslücken zu zeigen).

2.7 Ergebnis (Ziffer 7 der RAHMENBEDINGUNGEN)

Nicht anders als bei der Pflicht, ein Prüfungsprogramm zu erstellen, ist es auch erforderlich, der Prüfstelle vorzugeben, wie ihr Ergebnis auszusehen hat. Der Kontrollbericht muss die im Prüfprogramm aufgezählten Punkte umfassen und eine Gesamtbeurteilung enthalten. Er hat sich über die Erfüllung und den Erfüllungsgrad der Sollvorgaben zu äussern. Bei Mängeln soll er Empfehlungen für Verbesserungsmassnahmen enthalten. Er muss der für die Anwendung verantwortlichen Stelle an einer Sitzung mündlich erläutert werden.

[11] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937; StGB; SR 311.0