

Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes

insbesondere zum Inhalt der Verfahrensbeschreibung und zu den technischen und organisatorischen Maßnahmen

Version 1.0. vom 24. Oktober 2006

Bremerhaven, 24.10.2006

Unser Zeichen: 10-500-03.06/2#1

Alle öffentlichen Stellen, die personenbezogene Datenverarbeitung betreiben, haben Vorkehrungen zu treffen, um den Datenschutz sicher zu stellen. Hierzu sind besondere Festlegungen zu treffen, die in einem Datenschutzkonzept nieder zu legen sind.

Das Datenschutzkonzept hat verschiedene Aspekte zu beachten, so sind z.B. gewisse Schutzziele zu erreichen und auch Sicherheitsaspekte zu berücksichtigen. Informationen, die die Funktionsfähigkeit oder den Datenschutz des Systems gefährden können, sind besonders schützenswert und dürfen daher nicht der Öffentlichkeit zugänglich sein. Das Gesetz verlangt in diesem Zusammenhang die Erstellung einer Verfahrensbeschreibung nach § 8 Bremisches Datenschutzgesetz (BremDSG) sowie die Festlegung der technischen und organisatorischen Maßnahmen nach § 7 BremDSG.

Die nachfolgende Orientierungshilfe enthält Vorschläge, wie und in welcher Form diesen verschiedenen Zielen entsprochen werden kann.

Verfahrensbeschreibung nach § 8 BremDSG

Jede öffentliche Stelle ist verpflichtet, in einer Beschreibung für jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden, die dem Gesetz zu entnehmenden Festlegungen zu treffen. Das Gesetz verlangt dabei, dass die Beschreibungen ständig auf dem neuesten Stand zu halten sind (§ 8 Abs.2 BremDSG) und dass dem behördlichen Datenschutzbeauftragten die Verfahrensbeschreibung und eine Darstellung der Zugriffsberechtigungen unverzüglich, jedenfalls aber vor der Einführung oder vor wesentlichen Änderungen eines Verfahrens zu übersenden sind (§ 8 Abs.3 BremDSG).

Die Verfahrensbeschreibung dient u. a. folgenden Zwecken:

- der Einsichtnahme durch jedermann auf Anfrage
- als Grundlage zur Durchführung der (Vorab-)Kontrolle durch den behördlichen Datenschutzbeauftragten
- der klaren Festlegung der technischen Komponenten und ihrer Umgebung
- der genauen Bestimmung der personenbezogenen Datenverarbeitung in allen Phasen
- der Beschreibung der Zugriffsberechtigten und ihrer Rechte
- der Transparenz und Nachprüfbarkeit der personenbezogenen Datenverarbeitung.

Der § 8 Absatz 3 Satz 2 BremDSG sieht vor, dass Verfahrensbeschreibungen von jedermann bei der verantwortlichen Stelle eingesehen werden können. Kritisch können hier insbesondere die nach § 7 getroffenen technischen und organisatorischen Maßnahmen sein, soweit sie sicherheitsrelevante Informationen enthalten. Die Verfahrensbeschreibung selbst sollte daher lediglich für das Verfahren grundsätzliche und allgemeine Beschreibungen auf abstraktem Niveau enthalten. Dabei ist darauf zu achten, dass diese allgemeinverständlich sind, so dass sie bei Einsichtnahme vom Bürger verstanden werden können. Eine detaillierte Beschreibung über die konkrete Implementierung sowie die getroffenen technischen und organisatorischen Maßnahmen nach § 7 BremDSG soll getrennt von der öffentlich einsehbaren Verfahrensbeschreibung aufbewahrt werden.

Gesetzestext:

§ 8 BremDSG

Verfahrensbeschreibung und Meldepflicht

(1) Die verantwortliche Stelle ist verpflichtet, in einer Beschreibung für jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden, festzulegen:

- 1. Name und Anschrift der verantwortlichen Stelle,*
- 2. die Bezeichnung des Verfahrens und die Zweckbestimmung der Verarbeitung,*
- 3. die Art der verarbeiteten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,*

4. den Kreis der Betroffenen,
5. die Empfänger oder den Kreis von Empfängern, denen Daten mitgeteilt werden können,
6. Fristen für das Sperren und Löschen der Daten,
7. die technischen und organisatorischen Maßnahmen nach § 7,
8. eine geplante Datenübermittlung in Staaten außerhalb der Europäischen Union.

Die verantwortliche Stelle kann die Angaben nach Satz 1 für mehrere gleichartige Verfahren in einer Verfahrensbeschreibung zusammenfassen.

(2) Die Beschreibung nach Absatz 1 ist laufend auf dem neuesten Stand zu halten.

(3) Die Verfahrensbeschreibung und eine Darstellung der Zugriffsberechtigungen sind dem behördlichen Datenschutzbeauftragten unverzüglich, jedenfalls aber vor der Einführung oder wesentlichen Änderung eines Verfahrens zu übersenden. Die Verfahrensbeschreibungen können bei den verantwortlichen Stellen von jedermann eingesehen werden. Das Einsichtsrecht ist ausgeschlossen, wenn durch die Einsichtnahme die öffentliche Sicherheit gefährdet oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereitet würden.

Die technischen und organisatorischen Maßnahmen (TOMs) nach § 7 BremDSG

Der § 7 Abs.3 BremDSG legt detailliert die von den öffentlichen Stellen und den von ihnen beauftragten Stellen zu treffenden Maßnahmen fest.

Das Bremische Datenschutzgesetz beschreibt im § 7 Absatz 4 Ziffer 1 bis 8 BremDSG die Anforderungen an die Gestaltung der Systemsicherheit, die mit den zu ergreifenden technischen und organisatorischen Maßnahmen erfüllt sein müssen. Vorrangige Schutzziele sind unter anderen Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Dazu müssen angemessene technische und organisatorische Maßnahmen entsprechend § 7 Absatz 4 Punkt 1 bis 8 BremDSG getroffen werden. Diese sind im Gesamtzusammenhang und in ihrer gegenseitigen Wechselwirkung im Rahmen einer Sicherheitsarchitektur darzustellen.

Bei kleineren Organisationseinheiten und einer geringen Anzahl von eingesetzten Verfahren bietet sich die Erstellung eines Gesamtdatenschutzkonzeptes an. Bei größeren Organisationseinheiten und einer großen Anzahl von verschiedenen und ggf. zentral gesteuerten Verfahren bietet sich eine Aufteilung in ein Rahmendatenschutzkonzept und in Fachdatenschutzkonzepte an. Rahmendatenschutzkonzept, Fachdatenschutzkonzept und Gesamtdatenschutzkonzept sind aufgrund detaillierter sicherheitsrelevanter Informationen nicht öffentlich einsehbar. Einsicht besteht nur in die öffentliche Verfahrensbeschreibung. Dies gilt grundsätzlich auch nach den Regelungen im Informationsfreiheitsgesetz.

Gesetzestext:

§ 7 BremDSG

Datenvermeidung, Vorabkontrolle, technische und organisatorische Maßnahmen

(1) Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und der Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, haben die verantwortlichen Stellen zu untersuchen, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Die zu treffenden technischen und organisatorischen Maßnahmen sind zu dokumentieren. Das Ergebnis der Untersuchung ist dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten (Vorabkontrolle). Der behördliche Datenschutzbeauftragte hat sich in Zweifelsfällen an den Landesbeauftragten für den Datenschutz zu wenden.

(3) Die verantwortlichen Stellen und ihre auftragnehmenden Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung zu gewährleisten. Erforderlich sind Maßnahmen, soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Nach Maßgabe des Satzes 2 sind die Maßnahmen dem jeweiligen Stand der Technik anzupassen.

(4) Werden personenbezogene Daten automatisiert verarbeitet, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, der Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beispiel:

Während in der Verfahrensbeschreibung zur Zugriffskontrolle auf abstraktem Niveau formuliert wird, dass über eine differenzierte Rechtevergabe gewährleistet ist, dass nur berechtigte Personen an für sie zu bearbeitende Daten gelangen, wird im Fachdatenschutzkonzept das Beantragungs- und Genehmigungsverfahren zur Erlangung von Berechtigungen, die technische Umsetzung (z.B. Rollen, Profile), die Art der Implementierung (z.B. auf Anwendungs- oder auf Datenbankebene) sowie das Berechtigungskonzept selbst in seiner Ausprägung dargestellt.

Der im Anhang befindliche „Punktecatalog“ bietet einige Beschreibungen, die beispielhaft verdeutlichen, was inhaltlich jeweils mit den Maßnahmen gemeint sein kann. Eine differenzierte Betrachtung der einzelnen Fachverfahren und geeignete Umsetzung der Anforderungen aus dem § 7 BremDSG ist aber dennoch in jedem Fall erforderlich. Eine vollständige Auflistung von möglichen Maßnahmen kann an dieser Stelle nicht erfolgen, da sie in Abhängigkeit von den eingesetzten Informations- und Kommunikationstechnologien sehr unterschiedlich sein können. Außerdem lassen sich einige Technologien nicht eindeutig einem Schutzziel zuordnen, da sie mehrere Aufgaben erfüllen können.

Rahmendatenschutzkonzept der TOMs

Das Gesetz bietet die Möglichkeit, dass die verantwortliche Stelle die Angaben nach § 8 Abs.1 Satz 1 BremDSG für mehrere gleichartige Verfahren in einer Verfahrensbeschreibung zusammenfassen kann. Das gleiche gilt natürlich auch für die TOMs nach § 7 BremDSG: Diese Zusammenfassung kann allerdings nur für bestimmte Schutzziele erfolgen, die bezogen auf eine Dienststelle oder Behörde für alle Verfahrensbeschreibungen auf technischer Ebene bei der Verwendung gleicher Sicherheitsmechanismen identisch sind. Diese Maßnahmen lassen sich in einem übergreifenden Dokument für die betreffende Behörde bzw. Dienststelle (Organisationseinheit) zusammenfassen. Dieses Dokument wird als Rahmendatenschutzkonzept bezeichnet. Inhaltlich können die Zutrittskontrolle, die Zugangskontrolle, die Verfügbarkeitskontrolle sowie die Netzinfrastruktur und Netzsicherung und hier insbesondere die eingesetzten Sicherheitskomponenten als Teil der Weitergabekontrolle zur Beschreibung im Rahmendatenschutzkonzept in Frage kommen. Ebenso sollten dort auch allgemeine organisatorische Maßnahmen (Verpflichtung nach dem Bremischen Datenschutzgesetz, Schulungsmaßnahmen der Mitarbeiter zum Thema Datenschutz, Dienstanweisungen etc.) aufgeführt werden. Das Rahmendatenschutzkonzept ist immer durch die Fachdatenschutzkonzepte für die angewandten Fachverfahren zu ergänzen.

Fachdatenschutzkonzept der TOMs

Das Fachdatenschutzkonzept enthält alle Maßnahmen, die sich speziell auf die Anwendung beziehen (z.B. Regelungen der Zugriffe über ein Berechtigungskonzept). Unter Anwendung kann sowohl ein konkretes Softwareprodukt/Programm wie aber auch ein Prozess mit mehreren Funktionen verstanden werden.

Gesamtdatenschutzkonzept der TOMs

Sofern eine Zusammenfassung der Maßnahmen mit allgemeinem und übergreifendem Charakter nicht notwendig ist (z.B. weil in der entsprechenden Organisationseinheit nur eine einzige Anwendung zum Einsatz kommt), werden alle notwendigen Maßnahmen in einem einzigen nicht öffentlichen Gesamtdatenschutzkonzept zusammengefasst.

Die nachfolgende Grafik enthält alle Elemente, die ein Datenschutzkonzept enthalten soll. Es beschreibt die öffentlich zugängliche Verfahrensbeschreibung und die nicht öffentlich zu machenden detaillierten Angaben zu den TOMs.

Datenschutzkonzept

Öffentlich

„Verfahrensbeschreibung nach § 8 BremDSG“

1. Verantwortliche Stelle...
2. Name und Anschrift...
3. Art.. und Rechtsgrundlage...
4. Kreis der Betroffenen...
5. Empfänger...
6. Fristen...
7. Die technischen und organisatorischen Maßnahmen nach § 7 BremDSG

An dieser Stelle erfolgt eine allgemeinverständliche, vollständige, aber abstrakte Beschreibung der nach § 7 BremDSG getroffenen Maßnahmen, ohne dass hierbei sicherheitsrelevante Informationen verwendet werden.

8. eine geplante Datenübermittlung in Staaten außerhalb der Europäischen Union

Nicht öffentlich

Alternative A

Rahmendatenschutzkonzept der TOMs

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele mit allgemeinem und übergreifendem Charakter.

Fachdatenschutzkonzept der TOMs zum Verfahren

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele speziell für die Fachanwendung.

Alternative B

Gesamtdatenschutzkonzept der TOMs

Detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für bestimmte Schutzziele speziell für die Fachanwendung sowie eine detaillierte Beschreibung der Maßnahmen und deren konkrete Implementierung für Schutzziele mit allgemeinem und übergreifendem Charakter.

„Punktecatalog“

Zutrittskontrolle

Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Zugangskontrolle

Mit Zugangskontrolle ist die Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpassword, Benutzererkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von Call-Back-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Zugriffskontrolle

Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Weitergabekontrolle

Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Eingabekontrolle

Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Auftragskontrolle

Sofern personenbezogene Daten im Auftrag verarbeitet werden, richtet sich diese nach § 9 BremDSG. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung.

Verfügbarkeitskontrolle

Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Trennungsgebot

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann durch logische und physikalische Trennung der Daten gewährleistet werden.