ETAT DE FRIBOURG
STAAT FREIBURG

Kantonale Behörde für Öffentlichkeit und Datenschutz
Chorherrengasse 2, 1700 Freiburg

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Kantonale Datenschutzbeauftragte

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/odsb

—

Referenz:
E-Mail: secretariatatprd@fr.ch

Themenblatt 9

WEBSITES MIT ZUGRIFFSKONTROLLE

Memorandum für die Erstkontrolle

1. Zweck

Dieses Memorandum stützt sich auf *Beratungsbefugnis* der Datenschutzbeauftragten (Art. 31 Abs. 2 Bst. b des Gesetzes vom 25. November 1994 über den Datenschutz, DSchG) und auf die Aufgabe der Kantonalen Aufsichtsbehörde für Datenschutz, *im Voraus* zu allen Projekten *Stellung zu nehmen*, die die Verbreitung von besonders schützenswerten Personendaten auf einer Website vorsehen (Art. 8 Abs. 3 der Verordnung vom 3. Mai 2005 über die Websites des Staates). Das Memorandum soll den öffentlichen Organen *helfen*, die für die erforderliche vorgängige Stellungnahme erforderlichen Informationen bereitzustellen.

2. Allgemeines

2.1 Jedes öffentliche Organ, das Personendaten bearbeitet, ist für den Datenschutz *verantwortlich* (Art. 17 Abs. 1 des Gesetzes vom 25. November 1994 über den Datenschutz, DSchG[1], Art. 4 des Reglements vom 29. Juni 1999 über die Sicherheit der Personendaten, DSR[2]). Die auf einer Website mit Zugriffskontrolle veröffentlichten Informationen und Dokumente können von einer gewissen Anzahl von autorisierten Personen innerhalb und/oder ausserhalb des Informatiknetzes des Staates/des öffentlichen Organs eingesehen werden. Der Verfasser der Website muss sich immer bewusst sein, dass Daten, die auf einer Website mit Zugriffskontrolle veröffentlicht werden, weitgehend

[1] SGF 17.1
[2] SGF 17.1

zugänglich gemacht werden und sich damit ein Stück weit *seiner Kontrolle entziehen*, ohne dass er jedoch von seiner Verantwortlichkeit entbunden wird (Art. 17 Abs. 1 DSchG).

2.2. Die Verbreitung von Personendaten auf einer Website mit Zugriffskontrolle gilt als *Abrufverfahren* im Sinne von Artikel 2 Abs. 1 Bst. c DSR. Der Zugriff auf solche Daten darf nur gewährt werden, wenn eine **gesetzliche Bestimmung** dies vorsieht (Art. 10 Abs. 2 DSchG). Das öffentliche Organ muss insbesondere eine Risikobeurteilung vornehmen (Art. 8 DSR), die Zugriffsberechtigungen bestimmen (Art. 10 Abs. 2 DSR) und das Authentifikationsverfahren regeln. Das Abrufverfahren muss in einem Benutzerreglement dokumentiert werden, von dem eine Kopie der zuständigen Aufsichtsbehörde für Datenschutz zugestellt wird. Zu dessen Inhalt siehe Artikel 21 Abs. 3 DSR.

3. Sicherheitsmassnahmen

3.1 Die Informatiksysteme müssen den Standardanforderungen der *Informatiksicherheit* genügen (Art. 14 Abs. 1 DSR). Nach Artikel 17 Abs. 1 DSR muss der Zugriff auf Informatiksysteme, mit denen Personendaten bearbeitet werden können, durch Vorkehrungen geschützt werden, die ein Authentifikationsverfahren (Identifikation + Passwort) und ein Zugriffskontrollsystem umfassen (individuelle Zugriffsberechtigungen. Die **Weisungen** vom 16. Dezember 2002 der Finanzdirektion des Kantons Freiburg zur Passwortverwendung für die PCs beim Staat Freiburg sehen folgende Regeln vor:

a) ein *Authentifikationsverfahren*, das *mindestens die Identifikation* der Benutzerinnen und Benutzer sowie das Eingeben eines Passwortes mit *mindestens 7 Zeichen* beinhaltet,
b) regelmässige *Passwortänderung*,
c) die Passwörter müssen genügend komplex sein,
d) vor der Wiederverwendung eines Passworts muss dieses vorher *mehrmals geändert* worden sein,
e) ein *Zugriffskontrollsystem*, das auf einer Bestimmung individueller Zugriffs-berechtigungen beruht.

3.2 Je nach Sensibilitätsgrad der zur Verfügung gestellten Personendaten kommen auch noch weitere Massnahmen dazu (z.B. Verschlüsselung besonders schützenswerter Personendaten, Art. 20 DSR).

Dies sind also die wesentlichen Punkte für ein an die Kantonale Aufsichtsbehörde für Datenschutz gerichtetes Gesuch um Stellungnahme (Art. 8 Abs. 3 der Verordnung vom 3. Mai 2005 über die Websites des Staates). Die Informationen können entweder direkt in diesem Dokument in die entsprechenden Felder eingegeben werden oder in einem separaten Dokument aufgeführt werden. Falls nötig wird die Kantonale Aufsichtsbehörde weitere Auskünfte einholen.

4. Informationen für das Gesuch um vorgängige Stellungnahme an die Kantonale Aufsichtsbehörde für Datenschutz

4.1. Informationen über die Website und die bearbeiteten Daten

Name des verantwortlichen öffentlichen Organs Name der Website Zweck der Website Ist eine solche Veröffentlichung für die Erfüllung der gesetzlichen Aufgaben notwendig? Aus welchen Gründen (Art. 5 und 6 DSchG)?	
Beinhaltet die Website mit Zugriffskontrolle Personendaten? Welche (Art. 3 Bst. a DSchG)? Beinhaltet die Website mit Zugriffskontrolle besonders schützenswerte Personendaten? Welche (Art. 3 Bst. c DSchG)?	
Sind die betroffenen Personen informiert? Wie sind sie informiert worden? Wann sind sie informiert worden? Ist die Zustimmung dieser Personen eingeholt worden (Art. 10 DSchG)? Wie?	

4.2. Gesetzliche Grundlagen

Gibt es gesetzliche Grundlagen, die das Bearbeiten und die Veröffentlichung solcher Daten erlauben? Welche (Art. 4 DSchG)? Erlauben diese gesetzlichen Grundlagen den Zugang zu diesen Daten über ein On-line-Abrufverfahren (Art. 10 Abs. 2 DSchG)?	

4.3. Verantwortlichkeit

Name der für den Inhalt der Website verantwortlichen Person	

Ist eine gemeinsame Datenbearbeitung mehrerer Organe vorgesehen? Wenn ja, ist die Aufteilung der Verantwortlichkeiten schriftlich festgelegt worden (Art. 17 Abs. 2 DSchG und 6 DSR)?	

4.4. Zugriffsberechtigung

Ist bestimmt worden, wer zugriffsberechtigt ist? Ist der Umfang ihrer Zugriffsberechtigung festgelegt worden (lesen, kopieren, eingeben, ändern usw.) (Art. 10 DSR)[3]?	
Wenn besonders schützenswerte Personendaten bearbeitet werden, werden diese auf der Website mit Zugriffskontrolle in jedem Fall mit Zugriffs-berechtigung des Verantwortlichen veröffentlicht? Werden diese Zugriffsberechtigungen individuell erteilt? (Art. 21 Abs. 1 DSR)	
Gibt es eine schriftliche Verpflichtungserklärung der zugriffsberechtigten Personen, mit der sie sich zur Ein-haltung der Sicherheitsmassnahmen verpflichten?	

4.5. Sicherheit

Sind Sicherheitsmassnahmen getroffen worden? Welche (Art. 3 DSR)? Ist eine Risikobeurteilung vorgenommen worden (Art. 4 Abs. 2 DSR)? Welche? Ist ein Benutzerreglement vorgesehen worden (Art. 21 Abs. 3 DSR)? Gibt es schriftliche Richtlinien für die zugriffsberechtigten Personen (Art. 3 DSR)? Wir	

[3] Beispieltabelle im Leitfaden für die öffentlichen Organe – Datenschutzkonzept – Der Schutz von Personendaten in meinem Dienst, April 2006, Datenschutzbeauftragte des Kantons Freiburg.

bitten um Zustellung des Dokuments. Ist vorgesehen, dass regelmässig kontrolliert wird, ob die Benutzerinnen und Benutzer die Sicherheitsmassnahmen einhalten (Art. 4 Abs. 3 DSR)?	
Hat das für den Inhalt der Website verantwortliche Organ die geeigneten organisatorischen Massnahmen gegen jegliche unerlaubte Datenbearbeitung getroffen (Art. 22 DSchG)? Hat es die notwendigen organisatorischen und technischen Massnahmen getroffen (Art. 11 DSR)? Ist vorgesehen, dass diese Massnahmen überprüft werden (Art. 12 DSG)?	
Hat der zuständige Informatikdienst die geeigneten technischen Massnahmen gegen jegliche unerlaubte Datenbearbeitung getroffen (Art. 3 Abs. 1 DSR)? Sind Verschlüsselungsmassnahmen vorgesehen?	

4.6. Aufbewahren der Personendaten – Überwachung

Wie lange soll die Website mit Zugriffskontrolle bestehen?	
Ist bei unbestimmter Dauer eine periodische Überprüfung der Risiken und Massnahmen vorgesehen (Art. 12 DSR)?	
Ist die Aufbewahrung bzw. die Vernichtung der Personendaten vorgesehen? Sind bei elektronischer Archivierung Fristen für die Vernichtung der Daten vorgesehen worden? Was wird vernichtet? Alles? Auch die Sicherungskopien? Ist eine Wiederherstellung der Daten möglich?	
Sind Kontroll- bzw. Überwachungsmassnahmen vorgesehen?	

4.7. Private[4]

Ist ein Outsourcingverfahren vorgesehen (Hosting der Website mit Zugriffskontrolle durch einen externen Privaten)? ***Achtung***. *Ist dies der Fall, so ist der betreffende Private ebenfalls der Datenschutzgesetzgebung unterstellt (Art. 2 Abs. 1 Bst. b DSchG).*	
Ist das öffentliche Organ an einer von einem Privaten eingerichteten Website mit Zugriffskontrolle beteiligt? ***Achtung***. *Ist dies der Fall, so ist das öffentliche Organ ebenfalls der Datenschutzgesetzgebung unterstellt (Art. 2 Abs. 1 Bst. a DSchG).*	

[4] www.fr.ch/sprd unter: Weitere Informationen, Auftrag (Outsourcing)