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

Erläuternder Kommentar

zum Muster-Benutzerreglement für die Bekanntgabe von Personendaten durch Abrufverfahren

Dieses Musterreglement gründet auf der Beratungsbefugnis der Datenschutzbeauftragten (Art. 31 Abs. 2 Bst. b des Gesetzes vom 25. November 1994 über den Datenschutz, DSchG[1]). Es versteht sich als Orientierungshilfe zur Unterstützung der öffentlichen Organe von Kanton und Gemeinden bei der Einführung eines Abrufverfahrens. Es ist nicht vollständig und muss unter Berücksichtigung des konkreten Einzelfalls ergänzt werden.

Im Folgenden informieren wir Sie zuerst über die für ein Benutzerreglement *erforderlichen gesetzlichen Grundlagen* (1.) und dann über die einzelnen Punkte eines solchen *Reglements* (2.).

1. Zum Ingress – Gesetzliche Grundlagen

1.1 Art der gesetzlichen Grundlage

Hier stellt sich folgende Frage: Welche gesetzlichen Grundlagen sind erforderlich und was müssen sie beinhalten? Einige Bemerkungen:

> Zuerst einmal ist der *Verantwortliche der Datensammlung*, d.h. das für die Verabschiedung des Benutzerreglements zuständige Organ, anzugeben (Art. 3 Bst. g DSchG). Dieses Organ sollte im Ingress des Reglements aufgeführt werden, damit die Benutzerinnen und Benutzer wissen, wer das Reglement erlassen hat.

[1] SGF 17.1.

> Anschliessend müssen die *einschlägigen gesetzlichen Bestimmungen* (Art. 4 DSchG) bestimmt werden. Sie sollten aus Gründen der Klarheit und der Verständlichkeit ebenfalls im Ingress aufgeführt werden.

> Dann muss die *Art der erforderlichen gesetzlichen Grundlage* geprüft werden. So kann abgeklärt werden, ob die bestehenden gesetzlichen Grundlagen angemessen sind. Gemäss Artikel 10 DSchG darf der Zugriff auf Personendaten über ein Abrufverfahren einem Empfänger nur gewährt werden, wenn eine gesetzliche Bestimmung dies vorsieht. Mit anderen Worten: Es braucht eine Bestimmung in einem Gesetz oder einer Verordnung (bzw. einem Reglement), damit Zugriff über ein Abrufverfahren gewährt werden kann.

> Die Kantonale Aufsichtsbehörde für Datenschutz hat Artikel 10 Abs. 2 DSchG immer dahingehend ausgelegt, dass die gesetzliche Grundlage in einem *Gesetz* im formellen Sinn figurieren muss, wenn das Abrufverfahren *besonders schützenswerte* Daten betrifft (Art. 3 Bst. c und Art. 8 DSchG). Vgl. auch BGE 122 I 360 ff. In den übrigen Fällen genügt eine gesetzliche Grundlage im materiellen Sinn (Verordnung, Reglement).

> Schliesslich *definiert* das Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR)[2] das Abrufverfahren in Artikel 2 als automatisierten Datenbekanntgabemodus, dessen *Bedingungen* in Artikel 21 Abs. 3 DSR geregelt werden.

  Auf dieser Grundlage beruht das vorgeschlagene Muster-Benutzerreglement.

1.2 Inhalt der (formellen oder materiellen) gesetzlichen Grundlage

Nachfolgend einige Punkte, die in der gesetzlichen Grundlage geregelt werden sollten, die das Abrufverfahren vorsieht:

> In einem *Gesetz* kann man sich auf die *wichtigsten Punkte* beschränken, aufgrund deren dieses Thema auf Gesetzesstufe behandelt wird (z.B. Bearbeitung besonders schützenswerter Personendaten). Die *weiteren Einzelheiten* können im *Reglement* geregelt werden.

> Gemäss Artikel 2 Abs. 1 Bst. c DSR bedingt die Datenbekanntgabe durch ein Abrufverfahren, dass der Verantwortliche der Datensammlung eine *Zugriffsberechtigung* ausstellt. Die gesetzliche Grundlage sollte eine neutrale Formulierung enthalten (z.B. «Der Zugriff kann über ein Abrufverfahren gewährt werden...») oder vom Gesichtspunkt des Verantwortlichen der Datensammlung ausgehen (z.B. «X kann Y über ein Abrufverfahren Zugriff auf solche Daten gewähren»). Die umgekehrte Lösung unter dem Gesichtspunkt des Datenempfängers ist dagegen weniger geeignet (z.B. «Y kann durch ein Abrufverfahren auf die Daten von X zugreifen...»).

[2] SGF 17.15

> Der *Zweck* der Verwendung oder Wiederverwendung der Daten muss klar definiert werden. Wenn die gesetzliche Grundlage den Zweck nur allgemein umschreibt, muss das Benutzerreglement ihn genauer festlegen. Z.B.[3] Kontrolle der Personen, die die Bussen infolge Strafurteils wegen einer bestimmten Straftat bezahlt haben, im Hinblick auf die Erstellung einer Statistik für die Finanzdirektion.

> Das öffentliche Organ legt die *Aufgaben* der Verantwortlichen der Datensammlung und der Empfänger fest (Art. 10 DSR). Z.B.: Die Sicherheits- und Justizdirektion bestimmt, dass die Datensammlungen des Amtes für Strafvollzug zur Kontrolle der bezahlten Bussen X Mal pro Monat nachgeführt werden.

> Der Kreis der betroffenen *Empfänger* muss in der gesetzlichen Grundlage ausreichend definiert sein. Z.B.: Die Empfänger sind Mitarbeitende des Amtes für Statistik der Volkswirtschaftsdirektion.

> Die zur Erfüllung der Aufgabe erforderlichen *Datenkategorien* müssen präzisiert werden. Z.B.: Durch das Abrufverfahren bekannt gegeben werden Daten zur Identität der verurteilten Person, zur Art der Straftat, finanzielle Daten (Zahlungen).

2. <u>Zum Benutzerreglement</u>

Nachstehend zuerst einige allgemeine Bemerkungen, dann einige spezifische Bemerkungen zu den einzelnen Artikeln.

> Das Muster-Benutzerreglement dient als *Orientierungshilfe* für die Einführung einer automatisierten Datenbekanntgabe durch ein Abrufverfahren. Es kann geändert oder ergänzt werden, beispielsweise durch ein Schema oder eine Tabelle, das bzw. die festhält, wer wann auf welche Daten Zugriff hat.

> Je nach Vertraulichkeit der bekannt zu gebenden Daten und der Art ihrer Bearbeitung wird das Reglement *angepasst* oder *ergänzt*, damit es den Anforderungen des DSchG entspricht.

> Die *Varianten* in Artikel 1 sehen die Einführung eines Anhangs zum Reglement vor. Bei einer Änderung des Anhangs ist dasselbe Verfahren anzuwenden wie bei einer Änderung des Reglements.

> Konkret muss ein Benutzerreglement *mindestens* alle Punkte von *Artikel 21 DSR regeln*. Dies sind:

Art. 1 Verantwortlicher der Datensammlung und Empfänger

Abs. 1. Anzugeben sind das *verantwortliche Organ der Datensammlung* sowie Name und Funktion

[3] Die Beispiele sind fiktiv und setzen ein Gesetz im formellen Sinn voraus, das die Datenbekanntgabe durch ein Abrufverfahren erlaubt.

der *Personen, die für den Kontakt mit den Datenempfängern sowie für die Kontrollen zuständig sind*. Es ist auch möglich, die Namensliste im Anhang aufzuführen, wie dies die Variante vorsieht.

Abs. 2. Anzugeben sind die von der Bewilligung des Verantwortlichen der Datensammlung betroffenen *Empfänger* sowie die *Personen, die zum Zugriff auf die Daten befugt sind*, unter Angabe ihrer Funktion. Datenempfänger ist in der Regel ein öffentliches oder privates Organ. Es ist auch möglich, die Namensliste mit den zugriffsberechtigten Personen im Anhang aufzuführen, wie dies die Variante vorsieht.

Abs. 3. Der *Umfang des Zugriffs* muss präzisiert werden: Zugriff auf die ganze Datensammlung oder einen Teil davon, erlaubte Felder oder Informationen. Bei unterschiedlichen Zugriffsrechten empfiehlt es sich, die vorgeschlagene Variante zu verwenden und den Umfang der Zugriffsberechtigung der einzelnen Personen im Anhang anzugeben.

Art. 2 Zur Verfügung gestellte Daten

Abs. 1. und 2. Es ist zu präzisieren, um welche *Personendaten* es sich handelt (Art. 3 Bst. a DSchG), z.B.: Personalien wie Name, Vorname, Geburtsdatum und -ort, Adresse, Geschlecht, Zivilstand, Status in der Schweiz usw. und/oder *besonders schützenswerte Daten* (Art. 3 Bst. c DSchG), d.h.: religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, strafrechtliche oder administrative Sanktionen und diesbezügliche Verfahren. Zu vermerken ist auch, wenn keine besonders schützenswerten Personendaten zur Verfügung gestellt werden.

Abs. 3. Die *ungefähre Zahl der Personen*, über die die Datensammlung Daten enthält, ist zu vermerken.

Art. 3 Datenbearbeitung

Abs. 1. Das öffentliche Organ ist für die Daten verantwortlich und muss aus Sicherheits- und Effizienzgründen ermitteln, *wie oft* Daten bekannt gegeben oder abgerufen werden. Je nach Situation legt es insbesondere fest, wie oft oder in welchen Fällen Daten abgerufen werden dürfen, beispielsweise wenn die Daten nicht anderweitig beschafft werden können oder wenn sie für die Aufgabe des öffentlichen Organs unbedingt notwendig sind.

Abs. 2. Es entscheidet auch, ob die abgefragten Daten *ausgedruckt oder kopiert werden dürfen*. *Falls dies der Fall ist*, gelten für die nachfolgende Bearbeitung dieser Daten die allgemeinen Datenschutzgrundsätze, d.h. insbesondere Notwendigkeit einer gesetzlichen Grundlage, Verhältnismässigkeitsprinzip und Grundsatz der Zweckbindung (Art. 4, 5 und 6 DSchG). Die Bekanntgabe der Daten ist in den Artikeln 10 und 11 DSchG geregelt, während die Vernichtung und Archivierung der Daten Artikel 13 DSchG und Artikel 13 DSR untersteht. In der Praxis können diese Daten entweder verschiedenen bestehenden Datensammlungen zugeordnet oder zusammen abgelegt werden. Im zweiten Fall bilden sie eine eigenständige neue Datensammlung, die gemäss Artikel 19 DSchG bei der Kantonalen Aufsichtsbehörde für Datenschutz angemeldet werden muss.

Andernfalls müssen das formelle *Verbot*, Ausdrucke und Kopien zu erstellen, sowie die entsprechenden Sicherheitsmassnahmen aufgeführt werden.

Abs. 3. Die ***Empfänger*** sind nicht berechtigt, die Daten der Datensammlung zu ändern oder neue Daten einzugeben (Art. 21 Abs. 2 DSR). Wenn dies der Fall wäre, wären sie keine Datenempfänger in einem Abrufverfahren, sondern ***Beteiligte an einer Datensammlung***, die sich die Verantwortung mit deren Verantwortlichen teilen (Art. 3 Bst. h DSchG).

Art. 4 Authentifikationsverfahren

Das Authentifikationsverfahren muss mindestens die *Identifikation der Empfänger* durch die Eingabe eines persönlichen Passwortes beinhalten. Das Passwort muss regelmässig geändert werden. Diese Anforderungen sind mit den Bedingungen von Artikel 17 DSR vergleichbar.

Art. 5 Weitere Sicherheitsmassnahmen

Abs. 1. Hier sind die *allgemeinen und spezifischen Sicherheitsmassnahmen* des Organs anzugeben, das für die Datensammlung verantwortlich ist. Es geht darum, die organisatorischen und technischen Massnahmen festzulegen, um die Vertraulichkeit, Verfügbarkeit und Sicherheit der Daten zu gewährleisten. Mit diesen Massnahmen sollen insbesondere die Vernichtung von Daten, Diebstahl, der anonyme Zugriff, Fälschungen und jede andere widerrechtliche Verwendung oder unbefugte Bearbeitung verhindert werden. Es handelt sich beispielsweise um die Bearbeitung anonymer, kodierter oder verschlüsselter Daten.

Abs. 2. Der Begriff *«Protokollierung»* wird in Artikel 2 Abs. 1 DSR definiert. Die Protokollierung dient der Überprüfung (Art. 6), dass die Empfänger nur auf Daten zugegriffen haben, die sie benötigen.

Art 6 Kontrollmassnahmen

Hier sind die *Kontrollmassnahmen*, ihre Häufigkeit sowie das Kontrollorgan anzugeben, das über eine zweckgebundene Abfrage wacht. Die in Artikel 5 vorgesehene Protokollierung eignet sich besonders für diese Überprüfung.

Art 7 Mitteilung und Kopie des Reglements

Hier sind die allfälligen Empfänger einer *Kopie des Reglements* anzugeben, z.B. die Dienststelle, die Daten durch ein Abrufverfahren empfängt. Eine Kopie des Reglements ist der Kantonalen Aufsichtsbehörde für Datenschutz zuzustellen. Artikel 21 Abs. 3 DSR in fine sieht vor, dass eine Kopie des Benutzerreglements der kantonalen oder kommunalen Aufsichtsbehörde für Datenschutz zugestellt wird. Damit kann diese Behörde gegebenenfalls überprüfen, ob der Inhalt des Reglements mit den Datenschutzvorschriften vereinbar ist, und sich vergewissern, dass die Verwendung der Daten zu keiner widerrechtlichen Persönlichkeitsverletzung führt.

Zusätzliche Bemerkung

Gegebenenfalls empfiehlt sich eine Kostenanalyse, um abzuklären, ob ein Abrufverfahren in einem bestimmten Fall sinnvoll ist.

Anhang zum erläuternden Kommentar

Die wichtigsten allgemeinen gesetzlichen Grundlagen für die Erarbeitung eines Benutzerreglements sind:

Gesetz vom 25. November 1994 über den Datenschutz (DSchG) (SGF 17.1)

Art. 10 Bekanntgabe der Daten
a) Bedingungen

[1] …
[2] Der Zugang zu Personendaten über ein Abrufverfahren, namentlich ein On-line-Zugriff, darf einem Empfänger nur gewährt werden, wenn eine gesetzliche Bestimmung dies vorsieht.

Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR) (SGF 17.15)

Art. 2 Definitionen

[1] In diesem Reglement bedeuten die folgenden Ausdrücke:
a) …
b) *Protokollierung:* die Registrierung aller oder eines Teils der Aktivitäten, die auf einem Informatiksystem oder einer Informatikanwendung ausgeführt werden, zur Kontrolle oder Rekonstruktion;
c) *Abrufverfahren:* ein automatisierter Datenbekanntgabemodus, bei dem die Empfängerin oder der Empfänger der Daten aufgrund einer Bewilligung des Verantwortlichen der Datensammlung selber und ohne vorherige Kontrolle über den Zeitpunkt und den Umfang der Bekanntgabe entscheidet.
[2] …

Art. 21 *b) Abrufverfahren*
[1] **...**
[2] **...**
[3] Das Abrufverfahren muss in einem Benutzerreglement dokumentiert werden, das insbesondere Folgendes präzisiert: die Personen, die Zugriff auf die Daten haben, die verfügbaren Daten, die Abfragehäufigkeit, das Authentifikationsverfahren, die weiteren Sicherheitsmassnahmen sowie die Kontrollmassnahmen. Eine Kopie des Reglements wird der zuständigen Aufsichtsbehörde für Datenschutz zugestellt.