

Datenschutzforum Schweiz
c/o Ursula Uttinger
Hotzestrasse 35
8006 Zürich

Zürich 18. Mai 2007

Bundesamt für Justiz
3003 Bern

*Vernehmlassung zur Änderung der Verordnung zum Bundesgesetz über den
Datenschutz und zu einer Verordnung über die Datenschutzzertifizierung*

Sehr geehrte Damen und Herren

Gerne nehmen wir Stellung zu den beiden geplanten neuen Verordnungen.

Grundsätzlich begrüßen wir die Änderungen/Anpassungen und denken,
dass es in eine gute Richtung geht.

Verordnung zum Bundesgesetz über den Datenschutz

Art. 4 Abs. 1 lit. a und d:

Es stellt sich die Frage, inwiefern eine Verwirrung entstehen könnte. Es ist sehr wohl möglich, dass Adressdaten aus einem Telefonbuch oder anderen öffentlichen Quellen in die eigene Adressdatei gelangen. Diese Adressdatei müsste gemäss lit. a gemeldet werden, wenn die Daten für Akquisition genutzt wird, nicht jedoch wenn diese aus einer öffentlichen Quelle stammen. Ob jetzt diese Datensammlung gemeldet werden muss, geht nicht eindeutig aus der Verordnung hervor.

Art. 6 Abs. 2 lit. b:

Anbei werden die vom Gesetz geforderten „Datenschutzregeln, welche einen angemessenen Schutz gewährleisten“ zu „Datenschutzregeln, die

unverändert bleiben“ müssen. Es ist fraglich, ob es sich dabei nicht um weitergehende Pflichten geht, die in einem formellen Gesetz vorgegeben sein müssten. Es ist auch nicht einzusehen, warum die Regeln unverändert bleiben müssen, und es nicht genügt, dass der Schutz dem schweizerischen angemessen ist.

In den Erläuterungen wird zu Art. 5 noch darauf hingewiesen, dass der Datenschutzbeauftragte prüft, ob die „angegebenen Garantien und Schutzregeln“ ein angemessenes Schutzniveau aufweisen (vgl. auch Art. 31 Abs. 1 lit. e nDSG). In welcher Frist der Datenschutzbeauftragte tätig werden muss, ist aber nirgends hinterlegt. Es wäre zu begrüßen, wenn diese Fristen klar geregelt wären.

Art. 11:

Wir begrüßen, dass das Bearbeitungsreglement etwas klarer umschrieben wird.

Zum 5. Abschnitt: Datenschutzberater

Es sollte sowohl im Gesetz als auch in der Verordnung zwingend immer derselbe Ausdruck genutzt werden: Im Gesetz spricht man von „Datenschutzverantwortlichem“, in der Verordnung wird daraus der „Datenschutzberater“. Welche dieser zwei Bezeichnungen genutzt wird, ist – aus unserer Sicht - nicht relevant.

Art. 12 a Abs. 2

Von einem Datenschutzberater wird verlangt, dass er keine weiteren Tätigkeiten ausüben darf, die mit den Aufgaben des Datenschutzberaters unvereinbar sind. Wie dies sichergestellt wird, ist nicht definiert. Wird dies allenfalls vom eidg. Datenschutzbeauftragten kontrolliert?

Es wird auch verlangt, dass der Datenschutzberater über „die erforderlichen Fachkenntnisse verfügt“. Sinnvollerweise müsste man aber – ähnlich wie in der Zertifizierungsverordnung – auch diese Anforderungen bezüglich der Fachkenntnisse etwas klarer formulieren. Die heutige Formulierung, die nur von „erforderlichen Fachkenntnissen“ spricht, ist zu allgemein. Damit würde jede juristische Ausbildung ohne Weiterbildung im Datenschutz genügen. Wir sind der Auffassung, dass zumindest Nachweise von Teilnahme gewisser Kurse, Veranstaltungen o.ä. gefordert werden müsste, damit auch ein datenschutzrechtliches Wissen vorhanden ist.

Art. 12 Abs. 2 lit. b

Auch hier wird nur verlangt, dass der Datenschutzberater über die „erforderlichen Ressourcen“ verfügt. Allenfalls könnte in einem Anhang ein Richtwert der Stellenprozentage – im Verhältnis zu Anzahl Datensammlungen, Grösse der Unternehmens und Anzahl besonders schützenswerter Personendaten und/oder Persönlichkeitsprofile – definiert werden. Solche Anhaltspunkte könnten als Auslegungshilfen dienen. Ansonsten muss man auf erste Streitigkeiten und Urteile warten. Dies ist zu vermeiden.

Art. 18

Bundesorgane müssen im Gegensatz zu privaten Personen doch einige Datensammlungen nicht melden, unabhängig, ob sie eine Zertifizierung oder einen Datenschutzberater haben. Dies stellt ein gewisses Ungleichgewicht gegenüber privaten Personen dar, insbesondere, da die Privaten solche Datensammlungen melden müssen. Sinnvollerweise sollten Private und Bundesorgane nur unterschiedliche Meldepflichten haben, wo die Unterscheidung nachvollziehbar ist.

Verordnung über die Datenschutzzertifizierung

Einleitend: Varianten von Datenschutz-Qualitätszeichen

Aus Sicht der Konsumentinnen und Konsumenten ist ein einziges Datenschutz-Qualitätszeichen wünschenswert (ähnlich ISO 9001:2000). Ein Label-Wildwuchs wie im Bereich von Bio oder den verschiedenen Label bezüglich tiergerechter Haltung bei der Fleischproduktion ist nicht sinnvoll. Der Markt spielt ja in dieser Hinsicht, als verschiedene Zertifizierungsstellen akkreditiert werden können.

Die vorliegende Verordnung über Datenschutzzertifizierungen ist ungenügend; es geht nicht klar hervor, welche die Mindestanforderungen an eine Datenschutzzertifizierung tatsächlich sind. Die von der Arbeitsgruppe beim eidg. Datenschutz- und Öffentlichkeitsbeauftragten entworfene Regelung würde auch bezüglich Regeldichte genügen. Es ist nachvollziehbar, warum darauf verzichtet werden soll. Will man auf den Minimalanforderungen von Art. 4 und 5 bleiben, ist der Sinn und Nutzen einer Zertifizierung fraglich. Insbesondere wenn man die Anforderungen an die Qualifikation des Personals bei den Zertifizierungsgesellschaften damit vergleicht, muss man feststellen, dass dies nicht konsistent ist.

Art. 4 Abs. 3

Bei den Mindestanforderungen wird auf ISO 27001:2005 verwiesen. Es sollte beachtet werden, dass Informationssicherheit nur ein Teil des Datenschutzes

ausmacht. Insofern ist der Hinweis auf diese Norm zwar sinnvoll, aber absolut ungenügend. Der Datenschutz sollte im Zentrum stehen, insbesondere die datenschutzrechtlichen Grundsätze und die einzelnen Datensammlungen, und nicht die Informationssicherheit.

Anhang – Anforderungen an die Qualifikation des Personals der Zertifizierungsstelle

Wir begrüßen, dass an die Qualifikation des Personals hohe Anforderungen gestellt werden. Gleichzeitig müssen wir aber feststellen, dass diese Anforderungen nicht immer von allen Zertifizierungsgesellschaften gleich interpretiert werden. Gerade im Bereich des Praxisnachweises sollten die Zertifizierungsstellen streng überprüft werden. Es ist bekannt, dass Anwälte ihre Spezialgebiete nach wie vor selbst definieren können. Diese können zwar die Gesetze lesen und interpretieren, dies allein macht aber noch keine Datenschutzspezialisten. Dasselbe gilt auch bei den Zertifizierungsstellen: wenn Not an Personal ist, sind diese schnell bereit, eine Qualifikation anzuerkennen. Auch eine Ausbildung alleine dürfte in den meisten Fällen nicht genügen, um auf die datenschutzrechtlichen Probleme bei einem Audit zu stossen.

Allenfalls sollte man verlangen, dass die Auditoren/-innen gemeldet werden müssen.

Freundliche Grüsse

Datenschutz-Forum Schweiz
Ursula Uttinger
Präsidentin