Stellungnahme der ARGE DATEN vom 08.06.2011 zur:

DATENVERARBEITUNGSREGISTER-VERORDNUNG 2011 – DVRV 2011

Aufgrund umfangreicher eigener Erfahrungen mit Einsichten in das Datenverarbeitungsregister (DVR) ist der ARGE DATEN jede Maßnahme die den Einsichtsvorgang erleichtert, beschleunigt und kostenreduzierender gestaltet willkommen.

Der vorliegende Entwurf des Bundeskanzleramts zur Datenverarbeitungsregister-Verordnung 2011 (DVRV 2011) die die Datenverarbeitungsregisterverordnung 2002 (DVRV 2002) aufheben soll ist jedoch über weite Teile unausgereift und unbestimmt.

Fehlendes Sicherheitskonzept

Größter Mangel an der vorliegenden Verordnung sind fehlende Angaben zu technischen Sicherheitsmaßnahmen. Weder im Verordnungstext noch in den Erläuterungen werden Angaben darüber gemacht, welche Sicherheitsmaßnahmen ergriffen werden sollen um die geplante Internetanwendung „DVR-Online" sicher zu realisieren. Dies lässt befürchten, dass die DVRV 2011 gänzlich ohne umfassendes Sicherheitskonzept verfasst wurde.

So fehlen bereits grundlegende einfachste Sicherheitsanforderungen wie beispielsweise, dass auf „DVR-Online" nur über eine verschlüsselte Internetverbindung (per https-Protokoll) zugegriffen werden können soll. Die DVRV 2011 sollte daher den Betrieb einer sicheren Internetapplikation regeln, deren Sicherheit anhand von Zertifizierungen nach ISO 27001 bzw. ÖNORM A 7700 auch überprüfbar ist.

Fehlendes Datenschutzkonzept

Aufgrund weiterer fehlender Angaben ist aus dem Verordnungsentwurf auch nicht ersichtlich, wie die Daten des DVR zukünftig der Öffentlichkeit (technisch) zur Verfügung gestellt werden sollen. Sofern nämlich nicht entsprechende Sicherheitsmaßnahmen ergriffen werden, besteht die Gefahr, dass das DVR, welches eigentlich den Zweck erfüllen soll, Betroffene über die zu Ihrer Person verarbeiteten Datenarten zu informieren zum Datenlieferant für Adresshändler wird. Bisher wurden DVR-Registerauszüge bzw. DVR-Einlagebögen auf Anfrage hauptsächlich im PDF-Format zur Verfügung gestellt, in Sonderfällen wurden diese Unterlagen vom DVR jedoch auch als Bild-Datei oder Word-Dokument übermittelt. Das Auswerten dieser Dateien um an die Namen und Adressen von Sachbearbeitern zu kommen wäre zeit-/ und damit kostenintensiv gewesen und hätte sobald übermäßig viele DVR-Unterlagen angefordert würden entsprechende Aufmerksamkeit beim DVR erregt. Sollen die Daten in Zukunft online zur Verfügung gestellt werden, so könnte das DVR bei entsprechenden technischen Voraussetzungen für Adresshändler interessant werden die so legal – da die Daten der Öffentlichkeit zur Verfügung stehen – Namen, Adressen, Telefon- und Faxnummern sowie E-Mail-Adressen sämtlicher österreichischer Datenverarbeiter zuerst speichern und anschließend auch verkaufen könnten. Dies muss durch entsprechende technische sowie organisatorische Maßnahmen verhindert werden um das Vertrauen in das DVR und in weiterer Folge auch in die Datenschutzkommission (DSK) nicht zu zerstören. Dass der Schutz der Daten sowohl organisatorisch als auch technisch gewährleistet ist, könnte durch eine Zertifizierung gemäß European Privacy Seal (EuroPriSe) bzw. GoodPriv@cy sichergestellt werden.

Bezüglich der willkürlichen Verwendung von einmal veröffentlichten Daten ist es auch an der Zeit das Datenschutzgesetz entsprechend zu überarbeiten, sodass veröffentlichte Daten nur für einen, der Veröffentlichung entsprechenden, Zweck verwendet werden dürfen. Einhergehend mit einer Bestimmung die Datenverarbeiter dazu verpflichtet die Herkunft ihrer Daten lückenlos belegen zu können, ließen sich eine Unzahl aktueller datenschutzrechtlicher Probleme in den Griff bekommen.

Mangelnde Präzision der Einsichtsmöglichkeit ins DVR

Ein weiterer Punkt an dem die Unausgereiftheit des vorliegenden Verordnungsentwurfes deutlich erkennbar ist, ist bei einer der zentralsten Aufgaben des Datenverarbeitungsregisters – der Einsichtsmöglichkeit.

In § 5 Abs 1 DVRV 2011 wird abstrakt ein „öffentlicher" Zugang beschrieben. Gemeint ist dabei wohl ein öffentlicher Zugang per Internet zur geplanten Internetanwendung „DVR-Online". Über diesen sollen „öffentlich zur Verfügung stehende Daten des Datenverarbeitungsregisters" eingesehen werden. Eine Erklärung welche Daten „öffentlich zur Verfügung stehen" und welche „nicht öffentlich zur Verfügung stehen" (§ 5 Abs 2 DVRV 2011) fehlt. Aus der Verordnung sollte klar und eindeutig hervorgehen, welche Datenarten öffentlich zur Verfügung gestellt werden und welche nicht. Dies würde auch den Registrierungsvorgang für Datenverarbeiter transparenter gestalten, sofern nämlich eine Telefonnummer der Öffentlichkeit zur Verfügung gestellt wird, wird es für Datenverarbeiter ratsam sein eher eine Firmen- als eine Privattelefonnummer preiszugeben.

Obwohl der 7. Abschnitt der DVRV eine Meldung und Registrierung für den Fall regelt, dass die geplante „Internetapplikation DVR-Online" (über einen längeren Zeitraum) nicht erreichbar ist, fehlt eine manuelle Einsichtsmöglichkeit sowohl im Falle einer technischen Störung als auch ein allgemeines manuelles Einsichtsrecht. So kann und darf nicht davon ausgegangen werden, dass sämtliche Betroffene von denen persönliche Daten verarbeitet werden einen Internetzugang besitzen. So verfügten laut Statistik Austria im Jahr 2010 nur 72,9% der österreichischen Haushalte über einen Internetzugang.[1] Es muss also auch weiterhin ein manuelles Einsichtsrecht geben um sämtlichen Betroffenen die Möglichkeit zu bieten ins DVR Einsicht zu nehmen und so ihre Rechte zu wahren.

Mangelnde technische Präzisierung

Zahlreichen Passagen der DVRV mangelt es an einer technischen Präzision. Insbesondere wäre es von großer Bedeutung zu erfahren welche Systemanforderungen Benutzer erfüllen müssen um die geplante „Internetanwendung" nutzen zu können. So gibt es im Internet unterschiedlichste Technologien die teilweise proprietär sind, teilweise nur von bestimmten Internet-Browsern bzw. Betriebssystemen unterstützt werden und teilweise sogar ein Sicherheitsproblem darstellen könnten. Auch wenn sich Technologien, besonders im Internet, weiterentwickeln und rasch überholt sind, sollte die Verordnung grundlegende Richtlinien zur technischen Gestaltung von DVR-Online enthalten. Nur durch ein klares Bekenntnis zu quellenoffenen, Browser- und Betriebssystemübergreifenden Technologien

[1] Statistik Austria - Haushalte mit Internetzugang 2010 - http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/022214.html

welche darüberhinaus im Idealfall auch barrierefrei sein sollten, könnte sichergestellt werden, dass DVR-Online möglichst vielen Menschen zugänglich ist.

Gemäß Paragraph 9 haben Meldungen ans DVR elektronisch zu erfolgen. Auch Unterlagen sollen in elektronischer Form übermittelt werden. In welchem technischen Format (Bild-Datei, PDF-Datei, Text(Word)-Datei) dies zu erfolgen hat wird in der Verordnung nicht näher konkretisiert.

Unausgereifter Anmeldungsvorgang

Die Paragraphen 6 und 7 sehen eine Anmeldung mittels Bürgerkarte (§ 6) oder Benutzername und Passwort (§7) vor. Dass es dabei zwei Systeme zur Anmeldung geben soll, erscheint nicht sachdienlich und verursacht unnötige Kosten, da zwei unterschiedliche Systeme betrieben und gewartet werden müssen.
Zwar sieht bezüglich der Anmeldung bei der „Internetanwendung" § 17 Abs 1a DSG 2000 vor, dass diese durch die Bürgerkarte erfolgen kann. Eine Pflicht zur Authentifizierung mittels Bürgerkarte geht aus dem Gesetzestext jedoch nicht hervor. Aufgrund der derzeitigen geringen Verbreitung der Bürgerkarte sollte die Anmeldung mittels Bürgerkarte daher vorerst hintangestellt werden – bei einer entsprechenden Verbreitung in der Bevölkerung könnte „DVR-Online" jederzeit per Verordnung um eine Anmeldung mittels Bürgerkarte ergänzt werden.

Zur Überprüfung der, von einem noch nicht registrierten Benutzer der geplanten Internetanwendung „DVR-Online" angegeben Daten, sieht § 7 Abs 2 eine automatisierte Abfrage im zentralen Melderegister vor, dies soll anscheinend unrechtmäßige Anmeldungen verhindern. Aus den Erläuterungen zu § 7 geht jedoch hervor, dass sofern eine Überprüfung des Vor- und Nachnamens sowie der Postleitzahl und des Geburtsdatums im zentralen Melderegister positiv ist eine E-Mail mit Passwort an die vom Benutzer angegebene E-Mailadresse verschickt wird. Durch eine derartige Überprüfung lassen sich unrechtmäßige Anmeldungen jedoch nur bedingt verhindern, erfährt man Name und Postleitzahl doch aus dem Telefonbuch und müsste, um eine andere Person unrechtmäßig anzumelden, nur deren Geburtsdatum kennen. Würde es, wovon in der Regel zwar nicht ausgegangen werden muss, tatsächlich zu einer missbräuchlichen Anmeldung kommen, so würde die betroffene Person überhaupt nicht mitbekommen, dass unter ihrem Namen Datenanwendungen registriert wurden. Missbräuchliche Anmeldungen ließen sich daher nur verlässlich verhindern, falls bei der Anmeldung die gesamte Adresse des Benutzers mit dem Melderegister verglichen wird und das Passwort, zumindest per Einschreiben, an die Postadresse des Benutzers verschickt wird.

Paragraph 14 sieht im Fall der Registrierung einer Datenanwendung ebenfalls eine nicht näher beschriebene Benachrichtigung des entsprechenden Auftraggebers vor. Angaben darüber wie diese Benachrichtigung zu erfolgen hat fehlen sowohl im Verordnungstext als auch den Erläuterungen. Sofern der Registrierungsvorgang nicht entsprechend überarbeitet wird, sollte zumindest die Information, dass eine Datenanwendung registriert wurde, per Einschreiben erfolgen.

Technische Hürden für Datenverarbeiter

Gemäß Paragraph 21 ist eine Meldung an das DVR per E-Mail bzw. in nicht-elektronischer Form nur für registrierungspflichtige manuelle Dateien sowie bei einem länger als 48 Stunden andauernden technischen Ausfall vorgesehen. Bei dieser Regelung geht das Bundeskanzleramt anscheinend fälschlicherweise davon aus, dass aus der Tatsache dass jemand eine Datenanwendung (i.S.d. § 4 Z 7 DSG 2000 - dh. zumindest teilweise automationsunterstützt) betreibt geschlossen werden kann, dass dieser auch über Internet verfügt. Dadurch dass eine nicht-automationsunterstütze Meldung künftig nur noch in Ausnahmefällen vorgesehen sein soll, wird all jenen Datenverarbeitern die zwar eine Datenanwendung betreiben, nicht aber über eine Internetanbindung verfügen eine Registrierung durch eine unnötige technische Hürde erschwert. Eine manuelle Registrierung beim DVR zu ermöglichen ist nicht nur im Sinne der politischen Verantwortung, jedem Bürger ohne Rücksicht auf dessen technische und somit letztlich finanzielle Möglichkeiten, den Zugang zur Verwaltung zu ermöglichen, geboten, sondern würde darüber hinaus auch nur einen minimalen zusätzlichen Aufwand verursachen. Durch eine einfache und benutzerfreundliche Gestaltung der geplanten Internetanwendung „DVR-Online“ verbunden mit der Zeitersparnis die sich durch eine automationsunterstützte Registrierung ergibt würden Datenverarbeiter ohnehin motiviert ihre Datenanwendung(en) automationsunterstützt zu registrieren. Den zugegeben wenigen verbleibenden Datenverarbeitern die zwar eine Datenverarbeitung betreiben nicht jedoch über Internet verfügen[2] könnten analog zu denjenigen die eine registrierungspflichtige Datenanwendung betreiben die DVR-Formblätter auf Anfrage ausgedruckt zur Verfügung gestellt werden.

Bezüglich einer Meldung im DVR ist vorgesehen, dass diese neben Namen und Anschrift, auch Telefon-, Faxnummer sowie E-Mailadresse des Datenverarbeiters enthalten muss. Diesbezüglich sei zu bemerken, dass gerade in der heutigen Zeit, in der E-Mail immer mehr an Bedeutung gewinnt, während Fax an Bedeutung verliert, nicht davon ausgegangen werden darf, dass sämtliche Auftraggeber sowohl über eine Faxnummer als auch eine E-Mailadresse verfügen. Auftraggeber ohne Internetanbindung werden gar über keine E-Mailadresse verfügen, andere wiederrum verfügen vielleicht über keine Fax-Nummer mehr. Besonders bei einer automationsunterstützen Überprüfung von Angaben kann dies zu Problemen führen falls sämtliche Felder als Pflichtfelder gestaltet sind. So könnten Anträge aufgrund fehlender Angaben (automatisch) abgelehnt werden, bzw. Auftraggeber dazu verleitet werden Falschangaben zu machen.

[2] Im Jänner 2010 verfügte 1% der Österreichischen Unternehmen zwar über einen Computer, nicht jedoch über einen Internetzugang. Statistik Austria - Unternehmen mit Computereinsatz und Internetzugang im Jänner 2010 - http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_unternehmen_e-commerce/022195.html

Fazit

In Anbetracht der Unreife der vorliegenden Verordnung sowie dem Umfang der gemachten Anmerkungen erscheint ein Inkrafttreten mit 1.Juli 2011 als unrealistisch. Sofern man eine ausgereifte, getestete, den aktuellen Sicherheitsstandards entsprechende, anwenderfreundliche, möglichst barrierefreie Online-Applikation einführen möchte, ist sogar ein Inkrafttreten vor 1.1.2012 unrealistisch. Die Einführung einer unreifen, womöglich unsicheren DVR-Online Anwendung sollte jedenfalls vermieden werden um das Vertrauen in das DVR nicht zu verletzen.

ARGE DATEN

DB RECHT11229 / STELL / Unser Zeichen: DVRV_2011
per E-Mail: v@bka.gv.at

An das
Bundeskanzleramt
Abteilung Verfassungsdienst

Ballhausplatz 2
1014 Wien

Wien, 8. Juni 2011

Betreff: **BKA-810.127/0003-V/3/2011**
Stellungnahme der ARGE DATEN zur Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister **(Datenverarbeitungsregister-Verordnung 2011 – DVRV 2011)**

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme elektronisch übermittelt (v@bka.gv.at)

Eine Kopie der Stellungnahme wird weiters an folgende Adresse(n) verschickt:
☑ ronald.bresich@bka.gv.at [electronic mail]

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

ARGE DATEN - Österr. Gesellschaft für Datenschutz A-1160 Wien, Redtenbacherg. 20 ☎ +43/676/9107032, Fax +43/1/4803209
www.argedaten.at DVR 0530794 info@argedaten.at Gerichtsstand Wien
ZVR 774004629 UID ATU 56627966 PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)