schließlich gibt es noch den Bereich der Technikfolgenabschätzung zu neuen technischen Entwicklungen wie der ›allgegenwärtigen Computernutzung‹, zu Überwachungsinfrastrukturen oder zu Anonymisierungs- und Pseudonymisierungskonzepten [→].

Das ULD-i spricht nicht nur Unternehmensleitungen und das IKT-Management an, auch Betriebsräte können die Dienstleistungen des ULD-i nutzen, um die Entwicklung und den Einsatz von datenschutzgerechter Technik in ihrem Unternehmen zu initiieren.

Kai Janneck ist Diplom-Kaufmann und im Management des ULD-i tätig

www.uld-i.de/

Innovationszentrum Datenschutz & Datensicherheit (ULD-i)
Holstenstraße 98, 24103 Kiel
fon 04 31-988-13 99, kontakt@uld-i.de

Weitere Internetadressen:

www.datenschutzzentrum.de ***(Unabhängiges Landeszentrum für Datenschutz mit Informationen z.B. über das schleswig-holsteinische Datenschutz-Gütesiegel)***

www.anon-online.de/ ***(Anonymisierungsdienst für die Internetnutzung)***

www.datenschutz.de/ ***(das ›Virtuelle Datenschutzbüro‹)***

[→] Anonymisierung = IKT-Nutzung ohne Preisgabe der Identität

[→] Benutzungsoberfläche = die spezielle Art wie Informationen und Bedienungsmöglichkeiten einer Software auf dem Bildschirm präsentiert werden

[→] Datenschutz-Audit = Verfahren zur systematischen und regelmäßigen Überprüfung und Bestätigung (Zertifizierung) von Datenschutzmaßnahmen

[→] Identitätsmanagement = Handhabung/Organisation der Verwendung von Identitätsmerkmalen in der Informations- und Kommunikationstechnik (z.B. im Internet) etwa durch Anonymisierung/Pseudonymisierung

[→] Pseudonymisierung = IKT-Nutzung unter Verwendung eines ›Decknamens‹ (d.h. mit der Möglichkeit, unter geregelten Umständen den Bezug zu einer Person wieder herzustellen)

BRUNO SCHIERBAUM

Personendaten ins Ausland

Die bisherigen Datenschutzvorschriften für eine Übermittlung personenbezogener Daten in andere Staaten, vor allem auch in ›Drittstaaten‹ außerhalb der EU, sind durch neue Standardvertragsklauseln ergänzt und verbessert worden.

Zur Übermittlung personenbezogener Daten an Standorte außerhalb der Europäischen Union und zu den entsprechenden Vorgaben im Bundesdatenschutzgesetz (BDSG) ist in dieser Zeitschrift bereits ausführlich berichtet worden (siehe: ›Datenübermittlung ins Ausland – neue Vorgaben im BDSG‹ in cf 2+3/02). Dabei ging und geht es vor allem um ein vergleichbares Datenschutzniveau als Voraussetzung für den problemlosen Datenaustausch.

Die Umsetzung der EG-Datenschutzrichtlinie (dazu: ›EG-Datenschutzrichtlinie – die Frist läuft ab‹ in cf 10/98 ab Seite 24) hat in den Europäischen Staaten ein solches gleichwertiges, einheitliches Datenschutzniveau sichergestellt. Außerdem hat die EU-Kommission in der Zwischenzeit für bestimmte Länder außerhalb der EU festgestellt, dass auch dort ein angemessenes Datenschutzniveau besteht.

Dafür haben der Rat der Europäischen Union und das Europäische Parlament die EU-Kommission ermächtigt, auf der Grundlage des Artikel 25 Abs. 6 EG-Datenschutzrichtlinie zu entscheiden, ob ein ›Drittstaat‹ aufgrund interner Rechtsvorschriften oder eingegangener internationaler Verpflichtungen ein angemessenes (also den EU-Vorschriften vergleichbares) Datenschutzniveau gewährleistet. ›Drittstaat‹ meint jeden Staat außerhalb der Europäischen Union, eingeschlossen die drei Mitgliedstaaten des Europäischen Wirtschaftsraums (Island, Liechtenstein, Norwegen).

Eine solche Entscheidung der EU-Kommission setzt die Einhaltung folgender Bedingungen voraus:

- einen Vorschlag der EU-Kommission,
- eine Stellungnahme der Gruppe nationaler Datenschutzkommissare (der so genannten ›Art. 29-Datenschutzgruppe‹),
- eine durch qualifizierte Mehrheit der Mitgliedstaaten abgegebene Stellungnahme des ›Art. 31-Verwaltungsausschusses‹,
- Einhaltung einer 30-Tage-Prüfungsfrist, in der das Europäische Parlament feststellen kann, ob die Kommission ihre Ausführungsbefugnisse richtig angewendet hat (das Europäische Parlament kann, wenn es dies für angemessen hält, eine entsprechende Empfehlung abgeben),
- die Annahme der Entscheidung durch das Kollegium der Kommissionsmitglieder.

Die EU-Kommission hat bislang festgestellt, dass ein angemessener Schutz für personenbezogene Daten in der Schweiz, Kanada, Argentinien, Guernsey und Isle of Man gegeben ist, außerdem auch bei der Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des so genannten ›Sicheren Hafens‹ (›Safe Harbor‹) sowie bei der Übermittlung von Fluggastdatensätzen an die US-Zoll- und Grenzschutzbehörde.

Aktuell: Standardvertragsklausel

Aktuell hat die EU-Kommission jetzt noch eine neue Standardvertragsklausel für die Datenübermittlung in Nicht-EU-Länder verabschiedet. Die neue Klausel, die von mehreren Wirtschaftsverbänden gemeinsam vorgeschlagen wurde, ergänzt den bereits im Juni 2001 eingeführten Standardvertrag. Die jetzt geltenden Vertragsklauseln sind ein Instrument, mit dem Unternehmen und Organisationen auf unkomplizierte Weise ihrer Verpflichtung nachkommen können, vor einem Datentransfer sicherzustellen, dass bei der Übermittlung personenbezogener Daten in Nicht-EU-Länder ein ›angemessenes Datenschutzniveau‹ eingehalten wird.

Weitere Informationen und der Standardvertrag selber können über das Internet abgerufen werden:

http://europa.eu.int/comm/internal_market/privacy/modelcontracts_de.htm

In diesem Zusammenhang noch ein Hinweis: Wenn personenbezogene Daten von Beschäftigen entweder in Drittländer oder auch innerhalb der EU übermittelt werden sollen, sollten Arbeitgeber und Betriebsrat diesen Datentransfer zusätzlich durch den Abschluss einer Betriebsvereinbarung absichern. Der Arbeitgeber muss dann durch entsprechende Ergänzungen des mit den Datenempfängern abzuschließenden Standardvertrags gewährleisten, dass die Betriebsvereinbarung auch in den EU- oder Drittland-Unternehmen eingehalten und umgesetzt wird.

Bruno Schierbaum, ist als Berater für Betriebs- und Personalräte bei der Beratungsstelle für Technologiefolgen und Qualifizierung (BTQ) Niedersachsen tätig; Kontakt: BTQ Niedersachsen, Donnerschweer Str. 84, 26123 Oldenburg, fon 0441-8 20 68, **schierbaum@btq.de**

aus der praxis

datenschutztipps für die praxis

In dieser Serie werden regelmäßig Informationen und Praxisfälle zum Datenschutz veröffentlicht, wie sie in den Berichten der Datenschutzbeauftragten und Aufsichtsbehörden der Länder und des Bundes zu finden sind ...

HAJO KÖPPEN

Sicherheitsüberprüfungen, Einsatz von Filtersoftware

»Der sensible Umgang mit personenbezogenen Daten hat für viele private Unternehmen und Organisationen in Baden-Württemberg einen hohen Stellenwert. Es gibt aber auch einige Fälle von Datenmissbrauch und Gleichgültigkeit gegenüber datenschutzrechtlichen Regelungen und in einigen Bereichen grundsätzlichen Verbesserungsbedarf.« Mit diesen Sätzen leitete der Innenminister in Baden-Württemberg, Heribert Rech, seine Vorstellung des dritten Tätigkeitsberichts des Innenministeriums zum ›Datenschutz im nichtöffentlichen Bereich‹ für den Zeitraum Juli 2003 bis Juni 2005 ein. 914 Bürgerinnen und Bürger hatten im Berichtszeitraum bei der Datenschutzaufsicht um Unterstützung in Datenschutzfragen nachgesucht. Das ist eine Steigerung um 37 Prozent gegenüber den beiden Vorjahren – allein 50 Anfragen galten dem Arbeitnehmerdatenschutz.

1.

So baten Mitarbeiter einer Firma, die Dienstleistungen in Liegenschaften der US-Streitkräfte erbringt, die Datenschutzaufsicht um Unterstützung, weil sie sich vor ihrem Arbeitseinsatz einer Sicherheitsüberprüfung durch amerikanische Stellen unterziehen sollten (Seite 71). Dazu sollten sie ihr Einverständnis erklären, dass die US-Dienststelle in ihre Akten Einsicht nimmt und dass alle deutschen Sicherheits- und Polizeibehörden sämtliche über sie gespeicherte Daten an die amerikanische Dienststelle übermitteln (u.a. auch aus Akten über waffenrechtliche Erlaubnisverfahren).

Eine solche Generalermächtigung ging den Mitarbeitern doch etwas zu weit. Sie beklagten insbesondere, dass sie nicht wüssten, welche amerikanischen oder deutschen Stellen auf welcher Rechtsgrundlage welche Daten erheben und ob diese dabei auch in Akten Einsicht nähmen sowie von Vorgängen Kenntnis erhielten, die nach datenschutzrechtlichen Vorschriften nicht an andere deutsche Behörden, geschweige denn an amerikanische Stellen übermittelt werden dürften. Sie waren auch in Sorge, dass ihr Arbeitgeber auf diesem Weg Informationen erhalten könnte, zu denen er selbst sonst keinen Zugang hätte.

Zwischen der Datenschutzaufsicht und amerikanischen sowie britischen Dienststellen geführte Gespräche hatten schließlich Verbesserungen des Überprüfungsverfahrens zur Folge: »Es ist nunmehr klargestellt, dass die Sicherheitsüberprüfungen zwar von US-Streitkräften veranlasst, aber unter Federführung des Bundesamtes für Verfassungsschutz von deutschen Behörden auf der Grundlage des § 33 des Sicherheitsüberprüfungsgesetzes des Bundes durchgeführt werden. Die verwendete Einwilligungserklärung und der von dem Betroffenen auszu-