Forum
InformatikerInnen für
Frieden und gesellschaftliche
Verantwortung e.V.

FIfF e.V.
Goetheplatz 4
D-28203 Bremen
Tel. 0421 / 33 65 92 55
Fax 0421 / 33 65 92 56
fiff@fiff.de
www.fiff.de

Register ID 04361334865-55

Bremen, 15. Januar 2011

Stellungnahme des FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung zur EU-Konsultation zur Novellierung der Datenschutz-Richtlinie

In ihrer Mitteilung COM(2010) 609 vom 4. November 2010 kündigt die europäische Kommission an, die aus dem Jahr 1995 stammende Datenschutz-Richtlinie 95/46/EG zu novellieren und lädt dazu ein, im Rahmen einer Konsultation Vorschläge dazu einzureichen.

Als Hauptziele nennt die Kommission:

- Stärkung der Rechte der einzelnen Bürgerinnen und Bürger,
- Verbesserung des Binnenmarktes,
- Revision der Datenschutzbestimmungen bei der Zusammenarbeit von Justiz und Polizei bei der Strafverfolgung,
- Berücksichtigen der globalen Dimension des Datenschutzes,
- Verstärken der Institutionen, um Datenschutz besser durchzusetzen.

Wir begrüßen die Initiative zur Novellierung der Richtlinie. Zu einzelnen Aspekten des Datenschutzes nehmen wir im Folgenden Stellung und ersuchen die Kommission, die genannten Punkte bei der Novellierung zu berücksichtigen.

Zusätzlich verweisen wir auf die Stellungnahme der DVD – Deutsche Vereinigung für Datenschutz e.V. –, die wir ebenfalls unterstützen.

F.I.f.F.

1 Stärkung der Rechte der einzelnen Bürgerinnen und Bürger

Herstellung von Transparenz durch explizites Einverständnis zur Datenweitergabe – Opt-in statt Opt-out

- Heutige Regelungen sehen in einer Reihe von Fällen vor, dass der Einzelne der Weitergabe seiner personenbezogenen Daten aktiv widersprechen muss, wenn er sie ablehnt (z.B. beim Listenprivileg). Liegt kein Widerspruch vor, ist die Datenweitergabe in solchen Fällen zulässig. Damit dürfen Daten auch ohne das Wissen des Betroffenen weitergegeben werden. Dies lehnen wir ab. Das FIfF fordert, grundsätzlich das explizite Einverständnis des Betroffenen zur Voraussetzung der Datenweitergabe zu machen. Das Listenprivileg ist abzuschaffen.

- Zur Herstellung von Transparenz bei Weitergabe sind Dritte explizit zu benennen, Empfänger müssen sich die Zustimmung bestätigen lassen: Eine Weitergabe durch den für die Verarbeitung Verantwortlichen an Dritte soll zukünftig nur noch mit expliziter Zustimmung des Betroffenen erlaubt sein. Die Dritten müssen von den Verantwortlichen dazu soweit möglich explizit benannt werden, mindestens aber für die Zustimmung so weit spezifiziert werden, dass der Betroffene die Dritten mit zumutbarem Aufwand identifizieren kann, damit er auch diesen gegenüber bei Bedarf seine Rechte auf Auskunft, Löschung oder Berichtigung durchsetzen oder die Einwilligung zu einem späteren Zeitpunkt widerrufen kann. Der Empfänger (Dritte) muss gleichzeitig angemessen verifizieren, dass die Einwilligung tatsächlich vorliegt, um die Daten weiterverarbeiten zu dürfen. Dies könnte z.B. durch Anfrage beim Betroffenen oder Anfordern einer regelmäßigen Zertifizierung (Datenschutzaudit) der übermittelnden Stelle erfolgen.

Begründung:

- Sofern bisher überhaupt eine rechtskonforme Zustimmung für die Weitergabe eingeholt wird, werden oft in den vorformulierten Einwilligungserklärungen Dritte als Empfänger so pauschal benannt, dass der Betroffene diese Dritten nicht oder nur mit unverhältnismäßig hohem Aufwand identifizieren kann. Zudem kann ein Betroffener eine missbräuchliche Weitergabe der verantwortlichen Stelle nur schwer nachweisen, wenn die zulässigen Empfänger nicht genau genug spezifiziert sind.

- Ist die Zustimmung bzw. bei deren Fehlen der Missbrauch nicht klar definiert, fällt es auch dem Empfänger leichter zu postulieren, dass eine Zustimmung und damit eine legale Übermittlung vorliegt, auch wenn dies aus Sicht des Betroffenen gar nicht der Fall ist.

- Handelt es sich bei der verantwortlichen Stelle um eine Privatperson, die z.B. Daten von Bekannten weiter gibt, so kann die entsprechende Rechtskenntnis nur in den

seltensten Fällen vorausgesetzt werden. In einem solchen Fall darf die empfangende Stelle nicht mehr pauschal von einer legalen Weitergabe ausgehen. Ein Beispiel sind die Uploadfunktionen von persönlichen Adressbüchern bei der Anmeldung an sozialen Netzwerken, die den Benutzer geradezu verleiten, illegal Daten von Bekannten an die Betreiber weiterzugeben. Hier ist eine Bringschuld für Unternehmen erforderlich, die Auftragsdatenverarbeitung oder Erhebung von Daten Dritter durchführen. Diese sind dafür verantwortlich, sich davon zu überzeugen, dass die Einwilligung tatsächlich vorliegt.

Einwilligung zur Datenspeicherung im Internet

- Sofern die Zustimmung zu einer Datenspeicherung über das Internet übermittelten Daten nicht unmittelbar (innerhalb von 7 Tagen) erteilt wird, müssen die Daten ohne vorherige Weiterverarbeitung wieder gelöscht werden.

- Für die Erstregistrierung für Internet-Dienste muss das Closed-Loop-Verfahren verpflichtend werden. Im Gegensatz zum einstufigen Opt-in Verfahren, wird bei diesem Verfahren zweistufig verfahren. Ein Benutzer muss im ersten Schritt seine Angaben machen, welche Daten er z.B. zur Registrierung an einer Webanwendung oder Mailingliste speichern möchte. In der Folge bekommt er eine Bestätigungsmail an die angegebene Adresse, die neben den Daten, die gespeichert werden, einen Bestätigungslink enthält. Klickt der Nutzer diesen Link an, so wird der Nutzer auf eine Web-Seite geführt. Dort kann er Richtigkeit seiner Daten überprüfen und mittels eines Buttons bestätigen, dass er mit der Speicherung seiner Daten wirklich einverstanden ist.

- Mit diesem zweistufigen Verfahren wird erschwert, dass ein Nutzer wissentlich oder unwissentlich falsche Angaben macht, und dadurch einen anderen Nutzer anmeldet, der nicht möchte, dass seine Daten und seine E-Mail-Adresse in dieser Liste gespeichert werden. Sobald er die E-Mail erhält, mit der er aufgefordert wird, dem Link zu folgen, kann er durch einfaches Ignorieren der E-Mail verhindern, dass seine Daten persistent gespeichert werden. Der Anbieter der Anwendung ist verpflichtet, die Daten wieder zu löschen. Der Nutzer erfährt zum einen, dass irgendwer versucht hat, seine Daten bei einem Anbieter zu speichern und muss nicht umständlich erklären, dass er der Speicherung widerspricht.

Begründung:

- Bei einer Erstregistrierung kann der Zustimmende nicht eindeutig identifiziert werden. Deswegen kann bei einstufigem Opt-out nicht verifiziert werden, dass die Zustimmung tatsächlich von der registrierten Person stammt. Das Closed-Loop-Verfahren stellt diese Identität sicher.

Profilbildung über Menschen verhindern[1]

- Im Internet verbreitete Daten betreffen die Privatsphäre der Bürger und lassen das Erstellen umfangreicher Persönlichkeitsprofile zu. Sie müssen daher stark geschützt werden. Dies betrifft sowohl die Nutz- als auch die Bewegungsdaten.

Begründung:

- Die Zusammenführung von Daten ermöglicht zusätzliche Einblicke in die Privatsphäre der Bürger. Daher soll datenschutzrechtlich dafür gesorgt werden, dass auch jemand, der legal Zugriff auf mehrere Datenbanken hat, daraus für ihn nicht das Recht auf Zusammenführung der Daten folgt.

Befristete Einwilligung zur Datenspeicherung und -weitergabe

- Der Betroffene gibt seine Einwilligung nur befristet, eine Verlängerung erfordert eine aktive Erneuerung der Einwilligung.

Begründung:

- Die Häufigkeit der Fälle, in denen personenbezogene Daten verarbeitet werden, führt dazu, dass Betroffene schnell den Überblick verlieren können, wem sie Daten über sich selbst gegeben haben und erst recht, an wen diese ggf. weiter gegeben wurden. Zudem werden Daten häufig „vergessen“ zu löschen, wenn der ursprüngliche Zweck der Verarbeitung nicht mehr besteht, und zwar sowohl von der verantwortlichen Stelle als auch vom Betroffenen selbst, der der verantwortlichen Stelle vergisst mitzuteilen, dass etwas zu löschen ist oder dies wegen des Aufwands unterlässt. Die Einwilligung zur Datenspeicherung und Weitergabe sollte daher stets befristet sein, zumindest aber grundsätzlich bei der Einwilligung durch den Betroffenen befristet werden können.

- Dies wäre ein wichtiger Schritt in Richtung des aktuell diskutierten „digitalen Radiergummis“ für das Internet. Nach Ablauf einer vorgegebenen Frist verfällt das Einverständnis und Daten sind zu löschen, wenn keine Verlängerung explizit gewährt wird.

- Besonderes Augenmerk ist auf den Kinderschutz zu richten. Informationen, die von Minderjährigen angegeben wurden, müssen grundsätzlich gelöscht werden können, wenn sie selbst oder Erziehungsberechtigte dies einfordern.

Information über Datenweitergabe und deren Adressaten – Auskunftsrecht stärken

- Betroffene sind stets unaufgefordert zu informieren, ob, wann und an wen ihre Daten weitergegeben wurden („Datenbrief“). Dies gilt sowohl für den primären als auch für sekundäre Verwender der Daten. Die Information hat zu angemessenen

1 Quelle: CCC.

Zeitpunkten (mindestens einmal pro Jahr) in angemessener Weise zu erfolgen und muss selbst datenschutzkonform durchgeführt werden. Durch geeignete Verfahren ist sicherzustellen, dass sensible Daten durch den Datenbrief nicht in falsche Hände geraten.

- Das Recht auf Auskunft auf Anforderung des Betroffenen bleibt unberührt. Es muss grundsätzlich das Recht auf Auskunft in der eigenen Sprache bestehen.

- Um unnötigen Aufwand für Erstellung und Versand der Datenbriefe zu vermeiden, sollte ein Opt-out ermöglicht werden, durch den die Bürger auf die Zusendung des Datenbriefes verzichten können. Haben sich seit dem letzten Datenbrief keine Veränderungen ergeben, kann durch die Daten erhebende Stelle ebenfalls auf die Zusendung eines Datenbriefs verzichtet werden; denkbar wäre in solchen Fällen auch die Beschränkung auf eine kurze Mitteilung. Auf Anforderung ist jedoch stets die entsprechende Auskunft zu erteilen.

- Zu den personenbezogenen Daten müssen auch jene Daten und Informationen beigefügt werden, die ein Unternehmen aus den übermittelten oder aus anderen Quellen bezogenen Daten ableitet, d.h. im Rahmen des Profiling, Scoring oder bei der Ermittlung von „Vorlieben für bestimmte Produkte“ den ursprünglich übermittelten Daten hinzufügt. Dies ist die Mindestforderung, wenn eine Profilbildung nicht vollständig untersagt werden soll.

- Das Recht auf vollständige Auskunft soll nur mit unabhängiger richterlicher Prüfung eingeschränkt werden können.

Begründung:

- Die Versendung eines kostenlosen Datenbriefs soll mehr Transparenz für den Bürger bringen. Vor allem soll der Datenbrief eine Bringschuld des Unternehmens, der Behörde oder Institution sein, die personenbezogene Daten verarbeitet. Dies gilt vor allem deshalb, weil der Bürger oft gar nicht weiß, wer wie viele personenbezogene Daten von ihm verarbeitet.

- Profiling- und Scoringdaten müssen beigefügt werden, da zum Beispiel unrichtige Daten oder falsche Schlüsse/Scorings etc. eine Person stigmatisieren können. Zudem wird der Betroffene bei jedem Erhalt des Datenbriefs angeregt, darüber nachzudenken, ob er nach wie vor der weiteren Speicherung seiner personenbezogenen Daten zustimmt, oder es zum Anlass nimmt zu widersprechen.

- Der Mehraufwand, der für den Versand nötig ist, soll die verantwortlichen Stellen zur Datenvermeidung und Sparsamkeit motivieren.

Recht zur Verbandsklage bzw. Sammelklage

- Das Recht zur Klage in datenschutzrechtlichen Fragen ist auch Verbänden und Gruppen einzuräumen, die dieses Recht stellvertretend für Betroffene wahrnehmen.

Begründung:

- Kommerziell oder gar global operierende Anbieter können sehr leicht durch entsprechende Ausgestaltung ihrer Geschäftsprozesse die Rechte aller ihrer Kunden oder im Extremfall sogar großer Teile der Bevölkerung verletzen. Da es sich in solchen Fällen um Grundsatzfragen der Zulässigkeit einer Praxis handelt, ist es schon aus Effizienzgründen sinnvoll, solche Streitfälle rechtlich nicht als Einzelfallentscheidung vor überlasteten Gerichten zu behandeln. Zudem ist der Einzelne insbesondere bei Auseinandersetzungen mit Großunternehmen allein häufig nicht in der Lage, seine Rechte effektiv durchzusetzen. Durch den Mechanismus der Verbands- oder Sammelklage können Datenschutzrechte Betroffener effektiver durchgesetzt werden. Zum Beispiel könnte eine Arbeitnehmervertretung (Betriebsrat) stellvertretend für die Arbeitnehmer klagen.

Recht auf Anonymisierung und Verschlüsselung

- Jeder muss das Recht haben, anonym und verschlüsselt über öffentliche Netze zu kommunizieren. Verbot oder Einschränkung technischer Möglichkeiten der anonymen oder vertraulichen Kommunikation lehnen wir ab.

- Es ist zu gewährleisten, dass technische Schutzmöglichkeiten wie Verschlüsselung oder Anonymisierungsdienste (Privacy Tools) uneingeschränkt genutzt werden können. Insbesondere darf es grundsätzlich keine Einschränkungen zur Nutzung von starker Kryptographie oder einen Zwang zur Offenlegung von Kryptoschlüsseln geben. Diese werden nicht nur zur Anonymisierung und Verschlüsselung, sondern auch zur Absicherung der Datenintegrität benötigt, da Prüfsummen ebenfalls mit kryptographischen Mitteln gebildet werden.

- Ebenso müssen Anonymisierungsdienste und Verschlüsselungstechnologien grundsätzlich frei zugänglich sein und ihre Weiterentwicklung, Verbreitung und Betrieb nicht nur nicht behindert, sondern sogar öffentlich gefördert werden. Die Betreiber von Anonymisierungsdiensten wie z.B. Tor müssen einen besonderen Schutz vor Repressalien und Beschlagnahmung genießen, der eine hohe Eingriffsschwelle erzeugt.

Begründung:

- Zusätzlich zum Grundrecht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht 2009 im Urteil zur Online-Durchsuchung das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme formuliert.

- Auch für die Sicherung und Aufrechterhaltung weiterer Grundrechte wie u.a. Fernmelde- und Briefgeheimnis muss es grundsätzlich möglich sein, vertraulich zu kommunizieren. Für die Pressefreiheit und freie politische Willensbildung muss es grundsätzlich möglich sein, sich anonym im Internet zu informieren.

Verstöße gegen Datenschutzbestimmungen müssen angemessen sanktioniert werden

- Wir fordern, dass Bußgelder in einer Höhe verhängt werden können, mit der eine Gewinnabschöpfung analog §43(3) BDSG möglich ist.

- Um eine ausreichende Abschreckung zu gewährleisten, müssen verhängte Bußgelder sich analog dem Prinzip der Tagessätze an Umsatz und Gewinn der speichernden Stelle orientieren, also umso höher ausfallen, je größer der finanzielle Spielraum der speichernden Stelle ist. Durch diese Maßnahmen kann ein angemessener Abschreckungseffekt erzielt werden, der verhindert, dass Datenschutzverstöße vorsätzlich begangen oder billigend in Kauf genommen werden, da keine angemessene Sanktionierung zu befürchten ist.

- Eine Anzeigepflicht bei Verstößen muss allgemein (nicht nur für Telekommunikation) eingeführt werden, Verstöße gegen diese einzuführende Pflicht sollen zudem Straftatbestand werden.

- Die Einhaltung von Binding Corporate Rules (BCR) soll für das Unternehmen rechtlich bindend und für Betroffene einklagbar werden. (Unternehmensregeln werden durch die Selbstverpflichtung für dieses Unternehmen rechtlich bindend, analog von Betriebsvereinbarungen gemäß BetrVG im deutschen Arbeitsrecht.)

- Wenn ein Unternehmen wissentlich gegen Datenschutzgrundsätze und öffentlich gemachte Zusagen verstößt, die es sich selbst auferlegt hat, muss dies ebenfalls mit Bußgeldern oder sogar Gefängnisstrafe geahndet werden, da dadurch angenommen werden kann, dass der Betroffene arglistig getäuscht wird.

Begründung:

- Die Vergangenheit hat gezeigt, die bei Datenschutzverstößen verhängten Sanktionen nicht genügend abschreckende Wirkung entfalten, um wirksam zu sein. Darum fordern wir eine angemessene Sanktionierung solcher Verstöße.

- Die Veröffentlichung von Datenschutzvorfällen dient der Schadenreduzierung für die Betroffenen, da diese sich auf negative Folgen einstellen oder ausgleichende Vorsichtsmaßnahmen treffen können, z.B. Accounts sperren oder Passwörter wechseln. Gleichzeitig entsteht durch die mit der Veröffentlichung drohenden Imageverluste eine höhere Motivation der verantwortlichen Stellen für Prävention.

- Der Versuch einer Vertuschung eines Vorfalls soll eine strafbare Handlung werden und hat zum Ziel, das Risiko für die verantwortliche Stelle zu erhöhen, wenn sie dem drohenden Imageverlust zu entgehen versucht und damit höhere Risiken für die Betroffenen durch Unterlassen der Warnung in Kauf nimmt.

Durch Wahrnehmung seiner Datenschutzinteressen darf dem Betroffenen keine wesentliche Benachteiligung entstehen (Diskriminierungsverbot)

- Bestimmungen in Verträgen, AGB oder im Verwaltungsrecht, die zu einer unverhältnismäßigen Benachteiligung von Kunden oder Bürgern führen, die ihre Datenschutzinteressen wahrnehmen wollen, müssen untersagt werden.

- Wichtige, allgemein benötigte Dienstleistungen, müssen mit dem Prinzip der Datensparsamkeit und Vermeidung genutzt werden können. So muss es z.B. grundsätzlich möglich sein, Produkte oder Dienstleistungen bar zu bezahlen und es dürfen dabei keine wesentlich höheren Kosten entstehen als bei elektronischen Bezahlvorgängen. Eine allgemein benötigte oder nur von einem Anbieter verfügbare Dienstleistung (z.B. aufgrund eines Monopols oder sonstigen Mangels an datenschutzfreundlichen Alternativen) darf nicht durch eine Zustimmung zur Verwendung der Benutzerdaten durch Werbung finanziert werden. Es soll keine Verleitung oder Nötigung zur Angabe von Informationen geben, die für den eigentlichen Nutzungszweck nicht benötigt werden, um eine benötigte Dienstleistung nutzen zu können. Insbesondere wenn Alternativen fehlen, unverhältnismäßig teuer oder aufwendig sind, wird der Betroffene de facto dazu gezwungen, sein Grundrecht auf informationelle Selbstbestimmung aufzugeben und kann es nicht mehr frei ausüben.

Anwendungen, Hardware und Web-Dienste müssen standardmäßig restriktiv konfiguriert sein, beispielsweise bei Zugriffsrechten

- Geräte wie Smartphones, Router, etc. sind häufig so konfiguriert, dass sie über den Nutzer mehr Daten preis geben als für den Zweck des Dienstes erforderlich ist. Zum Beispiel wird bei Smartphones der aktuelle Standort genutzt, um Wetterbericht oder die nächste Pizzeria anzuzeigen. Diese Features werden dem Nutzer ungefragt zur Verfügung gestellt. Dass der Preis die Aufgabe des Schutzes auf Privatsphäre ist, ist den meisten Nutzern nicht transparent, ebenso wenig, dass sich von nun an ein Bewegungsprofil erstellen lässt. Die Dienste abzuschalten, ist oft umständlich und unterbleibt deswegen häufig.

- Deshalb müssen die Geräte datenschutzkonform ausgeliefert werden. Die Aktivierung eines Dienstes muss explizit durch den Nutzer erfolgen. Der Vorgang muss einfach zu handhaben sein.

- Zudem muss der Nutzer über die Konsequenzen informiert werden. Das heißt, ihm muss mitgeteilt werden, welche Daten für den Dienst von dem Anbieter abgerufen werden, und für welche Zwecke die Daten verwendet werden. Diesen weiteren

Zwecken darf ein Nutzer widersprechen, ohne das der Anbieter den Dienst verweigern darf. Untersagt ein Nutzer die weitere Verarbeitung, so muss der Anbieter die erhaltenen Daten sofort nach Diensterbringung wieder löschen, falls eine kurzzeitige Speicherung aus technischer Sicht erforderlich war. Ansonsten dürfen die Daten nur in einem flüchtigen Speichermedium verarbeitet werden.

- Es dürfen in jedem Fall (auch bei Erteilung einer Erlaubnis) nur jene Daten abgerufen werden, die für die Erbringung des Dienstes unabdingbar sind (strikte Zweckbindung). Alle Geräte müssen entsprechend vorkonfiguriert werden. Nötigenfalls müssen Geräte länderspezifische Konfigurationen anbieten.

- Für Software respektive Webanwendungen gilt das gleiche. Software muss stets Datenschutz konform ausgeliefert werden. Zum Beispiel müssen Webanwendungen wie soziale Netzwerke einen maximalen Schutz der Privatsphäre bieten.

- Bei Verlassen eines Netzwerkes müssen die personenbezogenen Daten für die anderen Teilnehmer des Netzwerkes unsichtbar gemacht werden. Die personenbezogenen Daten müssen nach einer angemessenen Frist vollständig gelöscht werden. Beiträge in Diskussionen müssen vorläufig, falls nicht ohnehin im Netzwerk üblich, pseudonymisiert werden. Nach einer angemessenen Frist müssen Beiträge/Diskussionen archiviert werden. Sie sind nur noch auffindbar, wenn man explizit wie in einem „echten“ Archiv danach sucht.

- Besonders zur Erzielung eines effektiven Kinderschutzes ist die datenschutzkonforme Konfiguration als Standard zu fordern.

Begründung:

- In den meisten Fällen werden sowohl Hardware als auch Software in einer Konfiguration ausgeliefert, der aus Datenschutzsicht bedenklich erscheint. Gleiches gilt für die initiale Konfiguration von Web-Diensten wie z.B. sozialen Netzwerken. Für unerfahrene Nutzer ist es häufig schwierig, sich einen vollständigen Überblick über die Konfiguration zu verschaffen und die Einstellungen entsprechend des von ihnen gewünschten Datenschutzniveaus vorzunehmen.

- Das führt häufig dazu, dass Nutzer unwissentlich Daten von sich preisgeben, vor allem, wenn sie fälschlich davon ausgehen, sich in einem geschützten, abgeschlossenen Kommunikationsraum zu befinden.

- Gerade bei Nutzern, die sich neu in einem Netzwerk anmelden oder sich neue Hardware kaufen, kann man Unerfahrenheit annehmen. Solche Nutzer quasi in ein offenes Messer laufen zu lassen, in dem alle Informationen, die sie zur Verfügung stellen, für alle Mitglieder oder auch weiterreichend sichtbar zu machen ist fahrlässig und unverantwortlich.

- Hiervon betroffen sind insbesondere Kinder, die von Natur aus offen und ehrlich sind und bereitwillig vieles ausplaudern, ohne, dass ihnen bewusst ist, dass jeder dies lesen kann. Deshalb müssen die Einstellungen restriktiv sein. Persönliche Daten dürfen nur explizit und dediziert freigegeben werden. Bei pauschalen Freigaben (alle Freunde) muss dem Nutzer angezeigt werden, wem er die Daten freigibt. Es muss die Möglichkeit geschaffen werden, weitere Einschränkungen zumachen. Zum Beispiel Freunde, die man persönlich (real) kennt, oder zusätzlich die Enge der Freundschaft beschreiben. In jedem Fall muss die Möglichkeit bestehen, pro Kontakt eine Freigabe dedizierter Daten zu bestimmen.

Datensparsamkeit und Datenvermeidung für Betreiber und Entwickler

- Wir fordern, dass bei der Entwicklung von IT-Systems die Prinzipien der Datensparsamkeit und Datenvermeidung verpflichtend werden. Am leichtesten lässt sich dies durchsetzen, wenn Anwendungen respektive Software so entwickelt wird, dass nur Daten durch die Anwendung erhoben und verarbeitet werden, die für den Zweck der Anwendung unbedingt erforderlich sind.

Begründung:

- Datensparsamkeit und Datenvermeidung sind wichtige Designprinzipien, die bereits bei der Entwicklung berücksichtigt werden müssen, da sonst ein datenschutzkonformer Betrieb nur noch mit erheblichem Aufwand möglich ist.

- In den letzten Jahrzehnten hat sich im Zuge der Verbilligung von Speichermedien eine Mentalität entwickelt, die die ehemals sorgsame Verwendung von Speicherplatz ins Gegenteil hat kippen lassen, nämlich möglichst viele Daten zu haben und zu verarbeiten, unabhängig davon, ob sie tatsächlich gebraucht werden. Frei nach dem Motto „vielleicht brauche ich die Daten ja doch noch“.

Datenschutzbildung verpflichtend machen

- Es müssen Mittel bereitgestellt werden, um Bildungsangebote zum Datenschutz und zu den Gefahren ungewollter Datenpreisgabe zu fördern. Dies umfasst beispielsweise Bildungsangebote zur Sensibilisierung für den Datenschutz (Awareness) und Nutzung von Privacy enhancing tools.

- Datenschutz ist in die Curricula an Hochschulen, Schulen, und berufliche Bildung aufzunehmen.

- Bei IT-nahen Berufen ist der Umfang solcher Angebote um Themen wie Datensparsamkeit und datenschutzgerechte Gestaltung von IT Systemen zu erweitern. In jeder Informatik- oder informatiknahen Ausbildung müssen die Prinzipien der Datensparsamkeit und Datenminimierung gelehrt werden.

Begründung:

- Das Bewusstsein, dass mehr Daten nicht zwangsläufig zu einer höheren Qualität des oder der Dienste führen, ist unterentwickelt, und führt dazu, dass Bürger, Staat und Unternehmen mehr Daten horten, als sie eigentlich bräuchten. Von daher wäre es dringend notwendig mittels Sensibilisierungskampagnen Bürger, Staat und Unternehmen darüber hinreichend aufzuklären und die in der IT tätigen über die Anforderungen und Verpflichtungen des Datenschutzes aufzuklären.

2 Verbesserung des Binnenmarktes

Verbot von nationalen Ausnahmen zur Vermeidung von Wettbewerbsverzerrungen

- Die EU-Datenschutzrichtlinie muss als Minimumstandard für Datenschutz in der gesamten EU etabliert werden. Mitgliedsstaaten dürfen nur strengere Auflagen machen, keine schwächeren Gesetze z.B. mit Ausnahmeregelungen für bestimmte Branchen, Produkte oder Dienstleistungen.

- Es darf keine nationalen Ausnahmeregelungen im Datenschutzrecht geben, die dazu führen, dass bestimmte Branchen, Produkte oder Dienstleistungen durch schwächere nationale Datenschutzbestimmungen billiger oder einfacher angeboten werden können als in Mitgliedsstaaten, in denen die Ausnahme nicht gilt und die EU Richtlinie konsequent umgesetzt wird. Ein schlechtes Beispiel dafür ist das Listenprivileg im deutschen Datenschutzrecht, das abgeschafft werden muss. Durch solche Ausnahmeregelungen kann schlechter Datenschutz zu einer Wettbewerbsverzerrung führen und sogar dazu anregen weitere Ausnahmen zu beschließen.

3 Revision der Datenschutzbestimmungen bei der Zusammenarbeit von Justiz und Polizei bei der Strafverfolgung

Datenverwendung grundsätzlich unter Richtervorbehalt

- Die Verwendung personenbezogener Daten durch Behörden – insbesondere Justiz- und Polizeibehörden – über den vorgegebenen Zweck hinaus ist grundsätzlich unter Richtervorbehalt zu stellen. Davon ausgenommen sind lediglich die auch sonst geltenden Regelungen (z.B. bei Gefahr im Verzug). Darüber hinausgehende Ausnahmetatbestände für Sicherheitsbehörden lehnen wir ab.

Unschuldsvermutung beachten

- Die Unschuldsvermutung ist bei jeder Datenerhebung durch Behörden strikt zu beachten. Datensparsamkeit muss auch für Ermittlungsbehörden gelten – auch und gerade bei der Strafverfolgung. Daten dürfen nur zweckgebunden und bei konkretem Verdacht erhoben werden. Eine verdachtsunabhängige Erhebung von Daten, wie bei der Vorratsdatenspeicherung (Data retention) vorgesehen, lehnen wir grundsätzlich ab. Die Richtlinie 2006/24/EG ist zurückzuziehen. Wir verweisen dafür auf das Urteil des Bundesverfassungsgerichts (1 BvR 256, 263, 586/08 vom 2. März 2010) und die einschlägigen Stellungnahmen, beispielsweise des Arbeitskreises Vorratsdatenspeicherung und des Chaos Computer Club.

- Wir verweisen auf die Empfehlungen im Rahmenbeschluss 2008/977/JI vom 27. November 2008, mit dem Ziel, „einen hohen Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Rechts auf Privatsphäre hinsichtlich der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI des Vertrags über die Europäische Union sowie gleichzeitig ein hohes Maß an öffentlicher Sicherheit zu gewährleisten.“ Wir regen an, die Empfehlungen dieses Rahmenbeschlusses bei der Novellierung der Datenschutzrichtlinie zu berücksichtigen.

4 Berücksichtigen der globalen Dimension des Datenschutzes

Aufrechterhaltung von internationalen Datenschutzstandards

- Für die Weitergabe personenbezogener Daten durch Behörden und Wirtschaftsunternehmen muss der gleiche Standard wie innerhalb der EU gelten. Dies ist im Einzelfall gegenüber den Datenschutzbehörden nachzuweisen. Das Safe-Harbour-Abkommen ist in seiner derzeitigen Form unzureichend und muss verbessert werden; insbesondere muss die Einhaltung angemessener Standards regelmäßig nachgewiesen werden.