Finanzkontrolle/Datenschutz
Datenschutzbeauftragter

Thurgau

Tätigkeitsbericht 2011 Datenschutzbeauftragter Kanton Thurgau

1 Vorwort

1.1 „E“ - Applikationen

Unser Zusammenleben wird heute zunehmend von verschiedenen zumeist webbasierten Diensten bestimmt, oder zumindest aber ergänzt. Der Austausch von Informationen in Menge und Geschwindigkeit nimmt immer noch rasant zu. Es eröffnen sich damit Möglichkeiten, die noch vor wenigen Jahren utopisch erscheinen.

Der Einzug dieser Tendenz macht auch vor den staatlichen Institutionen nicht Halt. Projekte mit dem Kürzel „E“ sind im Kanton Thurgau teilweise bereits in der Umsetzungsphase. Ausdrücke wie E-Health, E-Gouvernment, E-Gris, oder E-Vote sind längst etabliert. Mit der erhöhten technischen Machbarkeit von E-Projekten steigen die Anforderungen an den Persönlichkeitsschutz. Die Datenerhebung, die Datenhaltung, die Zugriffsrechte oder die Weitergabe von Personendaten müssen den gesetzlichen Vorgaben und dem verfassungsmässigen Recht der informationellen Selbstbestimmung genügen. Konsequenterweise müssen E-Applikationen transparent, nachvollzierbar und kontrollierbar aufgebaut sein. Daneben muss der betroffenen Person das Recht des Verzichts auf solche Dienste verbleiben. Vor dem Hintergrund der technischen Möglichkeiten von modernen Systemen kann ohne weiteres der Schutz der Persöhnlichkeit miteinbezogen und umgesetzt werden. Erforderlich ist jedoch das entsprechende Sensorium für die Belange unserer Bevölkerung. Die Wahrnehmung der Rechte des Einzelnen ist somit Pflicht und Aufgabe nicht nur der Datenschutzbeauftragten, sondern aller Behörden und beauftragten Dritten.

Frauenfeld, im März 2012

Ernst Frei
Datenschutzbeauftragter

2 Erläuterungen zu Cloud Computing

2.1 Einführung

Immer mehr Unternehmen und Behörden/Institutionen lagern ihre bisher typischerweise intern erledigten Datenverarbeitungen an externe Unternehmen aus («Outsourcing») und setzen dafür auf «Cloud Computing». Cloud Computing (deutsch: «rechnen in der Wolke») ist ein Begriff aus der Informationstechnik (IT). Er bedeutet, vereinfacht gesagt, dass Software, Speicherkapazitäten oder Rechnerleistung über ein Netzwerk, zum Beispiel das Internet, oder innerhalb eines Virtual Private Network (VPN) bedarfsorientiert bezogen, d.h. **gemietet werden**. Die IT-Landschaft (z.B. Rechenzentrum, Datenspeicher, Mail- oder Kollaborationssoftware, Entwicklungsumgebungen oder Spezialsoftware wie Customer Relationship Management [CRM]) steht nicht mehr im Eigentum des Unternehmens oder der Behörde und wird nicht mehr von diesen selbst betrieben, sondern von einem oder mehreren Cloud-Service-Anbietern **als Dienstleistung (Service) gemietet.** Die Anwendungen (und Daten) befinden sich nicht mehr im eigenen Netzwerk, sondern in der Cloud. Der Zugang zu Daten, Services und Infrastruktur, die in der Cloud zur Verfügung gestellt werden, erfolgt mittels Fernzugriff (remote access).
Die verschiedenen Varianten von Cloud Computing unterscheiden sich in Bezug auf Organisationsform und Servicemodell.

2.2 Organisationsformen

Es wird zwischen Private, Public, Hybrid und Community Cloud unterschieden.
In einer Public Cloud wird die Infrastruktur vollständig durch den Cloud Anbieter bewirtschaftet und bestimmt. Der Cloud-Nutzer hat diesbezüglich nichts zu sagen und kann beispielsweise keinen Einfluss auf die Serverstandorte nehmen. Anders dagegen die Private Cloud: Sie wird durch ein Unternehmen selbst oder durch einen externen Dritte betrieben und ist immer nur auf das jeweilige Unternehmen ausgerichtet. Eine solche Lösung ist viel sicherer, jedoch auch kostspieliger. Werden eine Public und eine Private Cloud gleichzeitig und parallel genutzt, spricht man von einer Hybrid Cloud. Eine Community Cloud schliesslich ermöglicht es verschiedenen Organisationen, dieselbe Infrastruktur gemeinsam zu nutzen.

2.3 Servicemodelle

Es gibt drei Typen von Servicemodellen: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) sowie Software as a Service (SaaS).

IaaS betrifft die Beherbergung: Der Cloud-Anbieter stellt in der Cloud einen Server zur Verfügung, auf dem die Cloud-Nutzer ihre Daten oder Anwendungen abspeichern können. Verantwortlich für das Funktionieren des Netzes, dessen Zugang, der Hardware etc. ist allein der Cloud-Anbieter. PaaS beschlägt die Bearbeitung von Daten: Der Cloud-Anbieter entwickelt eine Anwendung und stellt diese den Nutzern in der Cloud zur Verfügung. Die Bewirtschaftung der Daten mittels dieser Anwendung erfolgt jedoch durch den Nutzer selber. Bei SaaS ist der Cloud-Nutzer nur noch Konsument in der Cloud. Er bewirtschaftet nichts mehr selber, weder die Anwendungen noch die Daten. Ihm wird einzig in der Cloud eine Funktionalität zur Verfügung gestellt, um dort Daten bearbeiten zu können.

Die Hauptgründe für den Einsatz von Cloud-Computing-Systemen sind geringere Kosten für IT-Infrastruktur und Software, Software Updates on Demand, höhere Rechenleistung, dynamischer Speicherplatz (der gemietete Speicherplatz in der Cloud wächst oder schrumpft mit den Daten, die dort abgelegt werden), Mobilität, schnelle und einfache Verfügbarkeit, Skalierbarkeit und in einigen Fällen auch verbesserte und erhöhte Sicherheit.

2.4 Risiken bei der Nutzung von Cloud Computing

Die Auslagerung von Daten ist immer mit Risiken verbunden. Auf das Cloud Computing treffen insbesondere die folgenden zu:

2.4.1 Kontrollverlust über die Daten

Wegen der weltweiten Vernetzung und der Virtualität ist der Standort der Daten oft nicht erkennbar. Dies trifft im besonderen Mass für die Public Clouds zu. Der Cloud-Nutzer als verantwortlicher Dateninhaber weiss damit nicht, wo genau seine Daten in der Cloud gespeichert und verarbeitet werden. Er weiss oft auch nicht, ob Subunternehmer involviert sind und ob diese für einen angemessenen Datenschutz sorgen. Der Cloud-Nutzer kann somit seine datenschutzrechtlichen Pflichten hinsichtlich Gewährleistung der Datensicherheit, Gewährung des Auskunftsrechts oder Berichtigung und Löschung der Daten nicht (mehr) oder nur ungenügend wahrnehmen.

2.4.2 Fehlende oder mangelnde Abgrenzung/Isolierung der verschiedenen Datenverarbeitungen

Dem Konzept von Cloud Computing ist inhärent, dass verschiedene Nutzer, die in keiner Beziehung zu einander stehen, ihre Daten in derselben Cloud und durch dasselbe System verarbeiten lassen (sog. *Multi-Tenant-Architektur*). Damit erhöht sich das Risiko, durch Attacken auf einen der Nutzer in Mitleidenschaft gezogen zu werden. Die eigenen Daten könnten also wegen Hackerangriffen oder Distributed Denial of Services Attacken (DDoS) nicht mehr verfügbar sein oder selbst «mitgehackt» werden. Es ist deshalb eminent wichtig, dass die Datenbearbeitungen der verschiedenen Cloud-Nutzer strikt voneinander getrennt werden und es nicht zu einer Vermischung der Daten kommt.

2.4.3 Compliance Risiken

In der Cloud kann es vorkommen, dass Teile eines Datensatzes in verschiedenen weltweit verstreuten Rechenzentren liegen. Daraus ergeben sich Probleme nicht nur in Bezug auf die Gewährleistung von Datenschutz und Datensicherheit, sondern auch in Bezug auf die Einhaltung von anderen gesetzlichen Pflichten (Aufbewahrungs- oder Beweispflicht, Einhaltung von Geheimhaltungspflichten, etc.). Unternehmen und Behörden, die solche Dienste in Anspruch nehmen, sind sich oft zu wenig bewusst, dass die primäre Pflicht zur Einhaltung der Datenschutzregeln zunächst einmal bei ihnen selbst liegt und nicht beim Anbieter, der die Daten auf einem Cloud-Server speichert oder in der Cloud bearbeitet.

2.4.4 Zugriff von ausländischen Behörden auf die Daten

In vielen Fällen werden die Daten für die Bearbeitung in der Cloud ins Ausland bekannt gegeben. Dabei werden die Daten oftmals auch in Ländern gespeichert oder bearbeitet, die über keinen (ausreichenden) Datenschutz verfügen. Cloud–Service-Anbieter sind aber auch gegenüber ausländischen Behörden und Gerichten ver-

pflichtet, gegebenenfalls Zugriff auf Daten in der Cloud zu gewähren; dies gilt selbst dann, wenn die Daten nicht im Land der Behörde bearbeitet oder gespeichert werden.

2.4.5 Lock-in Effekte

Ein weiteres Risiko ist die Abhängigkeit vom Cloud-Service-Anbieter und fehlende Portabilität und Interoperabilität. Das heisst, die Daten können wegen nicht vorhandener standardisierter Technologien und Schnittstellen nicht (mehr) oder nur mit grossem finanziellem und/oder technischem Aufwand ins eigene IT-System zurückgeführt oder zu einem anderen Cloud-Anbieter migriert werden.

Die nachfolgenden Risiken bestehen immer, unabhängig davon, ob die Datenbearbeitung in einer Cloud stattfindet oder nicht.

2.4.6 Datenverlust

Daten können durch Diebstahl, Löschung, fehlerhafte Überschreibung oder sonstige Veränderung verloren gehen. Wenn keine entsprechenden Back-up-Systeme für die Originaldaten vorhanden sind, stellt dies ein enormes rechtliches Risiko dar und kann für ein Unternehmen möglicherweise existenzbedrohlich werden. Beispielsweise dann, wenn besonderes technisches Know-how, andere Geschäftsgeheimnisse (wie z.B. Kundenlisten oder Kalkulationsgrundlagen) oder die Finanzbuchhaltung betroffen sind. Zur Verhinderung von Datenverlusten müssen also entsprechende Sicherheitssysteme implementiert werden; solche Daten sollten nur zurückhaltend in die Cloud ausgelagert werden.

2.4.7 System- und Netzwerkausfälle sowie Nichtverfügbarkeit angemieteter Ressourcen und Services

Diese können dazu führen, dass Daten verloren gehen oder unberechtigten Personen zugänglich werden und damit die Vertraulichkeit, Sicherheit und Integrität der Daten nicht mehr gewährleistet ist. Überdies können solche Ausfälle den Geschäftsbetrieb eines Unternehmens oder der Behörde massiv beeinträchtigen und nebst finanziellen Verlusten auch gravierende Reputationsschäden nach sich ziehen.

2.4.8 Missbrauch der Daten durch böswillig agierende Insiders oder Mitarbeitende

Bei einem Outsourcing legt der Service-Anbieter unter Umständen nicht offen, wie die Zugriffsberechtigungen (physisch und virtuell) seiner Mitarbeitenden geregelt sind und wie diese diesbezüglich überwacht werden. Auch die Vertraulichkeitserklärungen sind für den Nutzer oft nicht einsehbar. Im Bereich Cloud Computing muss diesem Problem umso mehr Aufmerksamkeit gewidmet werden, wenn es um eine Public Cloud geht.

2.5 Datenschutzrechtliche Anforderungen bei der Nutzung von Cloud-Computing-Diensten

Werden bei der Nutzung von Cloud-Computing personenbezogene Daten bearbeitet, so liegt aus datenschutzrechtlicher Sicht normalerweise eine Datenbearbeitung durch Dritte im Sinne von Art. 10a DSG vor. Demnach kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten (hier: Cloud-Service-Anbieter) übertragen werden, wenn die Daten nur so bearbeitet werden, wie der Auftraggeber (hier: Cloud-Nutzer) selbst es tun dürfte, und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet. Der Cloud-Service-Anbieter muss also verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Anbieter beigezogen werden. Die Umsetzung dieses Erfordernisses bereitet in der Praxis jedoch Schwierigkeiten, da bei den Cloud-Computing-Anwendungen die Unterauftragsverhältnisse des Cloud-Service-Anbieters für den Cloud-Nutzer oft nicht transparent sind.

Weiter muss sich der Cloud-Nutzer vergewissern, dass der Cloud-Service-Anbieter als Dritter die Datensicherheit im Sinne von § 12 TG DSV gewährleistet. Das heisst, die Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Es muss für Vertraulichkeit, Verfügbarkeit und Integrität der Daten gesorgt sein. Der Cloud-Service-Anbieter muss die Daten gegen folgende Risiken schützen: unbefugte oder zufällige Vernichtung oder zufälligen Verlust; technische Fehler; Fälschung; Diebstahl oder widerrechtliche Verwendung; unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Diese Massnahmen sind periodisch vor Ort zu überprüfen. Wie die Datenschutzanforderungen im Einzelnen umzusetzen sind, hängt vom Unternehmen bzw. der Behörde, von der Art der Daten, aber auch von der Organisation und des Zuschnitts der Cloud-Lösung (bspw. Private oder Public; IaaS, PaaS oder SaaS) ab. Als Grundregel gilt: Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud, insbesondere eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-) Sicherheitsvorkehrungen und deren Kontrolle sein.

Die Nutzung von Cloud-Computing bedingt in vielen Fällen eine Datenbekanntgabe ins Ausland, da die Verarbeitung oftmals auf weltweit verstreuten Servern stattfindet. Häufig werden dazu auch Subunternehmer beigezogen. Sehr oft geht es dabei um Länder, die ein tieferes Datenschutzniveau als die Schweiz aufweisen, so dass mit der Übermittlung dorthin die Gefahr einhergeht, dass mit diesen Daten Bearbeitungen durchgeführt werden, die in der Schweiz nicht erlaubt wären. Aus diesen Gründen dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (§ 9a TG DSG). Unter diesen Umständen können Personendaten nur ins Ausland bekannt gegeben werden, wenn eine der in § 9a TG DSG aufgeführten Bedingungen erfüllt ist. In vielen Fällen wird der Cloud-Nutzer daher nicht umhin kommen, mit dem Cloud-Service-Anbieter (unter Einbezug allfälliger Subunternehmer) vertragliche Datenschutzgarantien abzuschliessen. Dabei besteht die praktische Schwierigkeit, dass alle Teilnehmer in der Cloud, auf deren Rechner personenbezogene Daten bearbeitet werden, vertraglich eingebunden werden müssen. Es ist zu bedenken,

dass grundsätzlich derjenige, welcher Personendaten ins Ausland übermittelt, nachweisen muss, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.

Schliesslich ist der Cloud-Nutzer auch dafür verantwortlich, dass das Auskunftsrecht nach § 20 TG DSG und das Recht auf Berichtigung nach § 22 TG DSG jederzeit gewährleistet sind und entsprechend den datenschutzrechtlichen Vorgaben umgesetzt werden. Die Einhaltung dieser Erfordernisse kann mit erheblichen Schwierigkeiten verbunden sein, da mit der Nutzung von Cloud-Anwendungen wie erwähnt oftmals ein Kontrollverlust über die Daten einhergeht und der Cloud-Nutzer nicht (mehr) weiss, wo welche Daten bearbeitet werden. Er kann sich von diesen gesetzlichen Pflichten jedoch nicht befreien.

2.6 Schlussfolgerung

Die sorgfältige Auswahl (inkl. Risikobeurteilung), Instruktion und Überwachung des Service-Anbieters sind zentrale Elemente bei einer Datenbearbeitung in der Cloud. Der Cloud-Nutzer bleibt als Auftraggeber letztlich gegenüber den betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und haftet bei allfälligen Verletzungen. Deshalb sollte er sich gut überlegen, welche Anwendungen und Daten er am eigenen Standort behalten will und welche in die Cloud wandern sollen. Zu diesem Zweck muss er im Vorfeld eine sorgfältige Prüfung des Cloud-Service-Anbieters und eine umfassende Risikoeinschätzung in organisatorischer, rechtlicher und technischer Hinsicht vornehmen. Bei der Auswahl der in Frage kommenden Cloud-Variante (Private Clouds, unternehmenseigene Public Clouds oder Hybrid Clouds) ist frühzeitig eine gründliche Analyse gerade auch der datenschutzrechtlichen Anforderungen vorzunehmen. Auf diese Weise kann von Beginn an eine datenschutzkonforme Gestaltung der Cloud gewährleistet werden. Besonderes Augenmerk sollte auf die Bearbeitung mit personenbezogenen Daten gelegt werden, was alle Schritte von der Speicherung über die Weiterverarbeitung bis hin zur Löschung mit einschliesst. Falls aufgrund der Risikoeinschätzung bezüglich der Verarbeitung von Personendaten in der Cloud Zweifel bestehen, ist von einer Auslagerung der Daten abzusehen.

3 Anonym surfen im Internet?

Ist es heutzutage möglich, beim Surfen im Internet anonym zu bleiben? Cookies beispielsweise werden immer leistungsfähiger, wenn es darum geht, Web-Browser zu personalisieren. Doch auch ganz abgesehen von dieser Technologie ist zu bemerken, dass der benutzte Browser selbst einen Abdruck hinterlässt, der uns eindeutig identifiziert. Diese Feststellung kann nach der Prüfung und Testanwendung des Algorithmus Panopticlick bestätigt werden.
Seit den Anfängen des Internet können wir mit Hilfe der Cookies bequemer surfen. Diese kleinen Dateien werden beim Besuch auf einer Website in unseren Computern abgelegt, speichern die Präferenzen des Nutzers (wie zum Beispiel die Sprache, in der eine Website angezeigt werden soll) und ermöglichen es so der Website, den Nutzer bei einem künftigen Besuch wieder zu «erkennen».
Über die Cookies-Technologie hinaus haben Forscher Folgendes festgestellt: Jeder Internet-Browser hinterlässt einen Abdruck, der einzigartig oder beinahe einzigartig ist. Somit braucht es keine Cookies mehr, um zu erkennen, welcher Computer sich

mit einer Website verbunden hat; es genügt, die Spur des benutzten Browsers zu beobachten.
Der von Electronic Frontiers Foundation angebotenen Algorithmus Panopticlick wurde geprüft und getestet (Panopticon ist ein Modellgefängnis, in dem die Wärter die Gefangenen unbemerkt beobachten können). Dieser Algorithmus betrachtet eine gewisse Anzahl Parameter bei der Eingabe und liefert ein Entropiemass, mit dem die Einzigartigkeit des getesteten Browsers bestimmt werden kann. Die Parameter sind zum Beispiel der «user agent», der Informationen über den Typ und die Version des Browsers, aber auch des verwendeten Betriebssystems liefert, die Liste der eingerichteten Plug-ins - wobei ein Plug-in eine kleine Software ist, die den Browser mit neuen Funktionalitäten wie etwa das Abspielen von Videos, die eingerichteten Schriftarten oder Informationen über den benutzten Bildschirm ergänzt. Tatsächlich werden sämtliche Informationen gesammelt, auf die man über den Browser zugreifen kann. Diese Informationen gelten aneinander gereiht als Identifikator (Abdruck) des Browsers. So bestimmt die mögliche Einzigartigkeit dieser Kennung die Eindeutigkeit des Browsers.
In der ersten Verbreitungsphase des Algorithmus wurden rund 400'000 solcher Identifikatoren gesammelt und anonymisiert. Jeder neue Abdruck wird mit dieser Sammlung abgeglichen, um festzustellen, ob er einem der bereits bekannten Abdrücke ähnlich ist. Ist dies der Fall, wird ermittelt, wie viele Abdrücke in einer Untergruppe enthalten sein müssen, um darin mit Sicherheit einen identischen Identifikator finden zu können.
Diesen Algorithmus mit den neuesten Versionen der bekanntesten Browser (Internet Explorer, Firefox, Chrome, Safari, Opera) unter verschiedenen Bedingungen wurde getestet: unmittelbar nach der Einrichtung des Browsers, nach einer gewissen Surf-Dauer, in anonymem Modus und nach Zufügung gewisser Erweiterungen.
Abschliessend wurde Folgendes festgestellt: Es muss tatsächlich eingeräumt werden, dass der Abdruck jedes Browsers einzigartig oder leicht identifizierbar ist. Es gibt indes Möglichkeiten, die Gefahren einer eindeutigen Identifikation etwas zu vermindern. So ist der anonyme Surf-Modus, der heute von sämtlichen Browsern angeboten wird (zumindest in ihrer neuesten Version) ein nützliches Tool. Gekoppelt mit gewissen Erweiterungen wie NoScript, die insbesondere vom Browser Firefox angeboten werden, ist er das beste Mittel zur Wahrung der Anonymität beim Surfen im Internet.

3.1 Neuentwicklung bei den Cookies

Im Rahmen verschiedener Beobachtungen im Bereich der Technologie wurde die Entwicklungen bei der Verwendung von Cookies untersucht. Cookies sind ein bei den Web-Browsern wohlbekannter Mechanismus, der es ermöglicht, die beim Surfen hinterlassene Spur des Nutzers zu speichern. Sie sind gewissermassen das Gedächtnis der Browser. Mit der technologischen Entwicklung sind diese Cookies, ursprünglich bloss kleine Textdateien, immer leistungsfähiger und damit eine eigentliche Bedrohung für die Privatsphäre geworden.
Ein Cookie ist die von einer Webseite beim ersten Besuch an den Browser gesandte kleine Datei, die bei jedem erneuten Besuch an die Seite zurück geschickt wird. So erkennt die Webseite den Browser und demzufolge den Computer und den Benutzer. Gewisse Präferenzen des Nutzers können gespeichert und durch die Webseite bei jedem weiteren Besuch reaktiviert werden.
Eine erste Weiterentwicklung waren die so genannten Drittanbieter-Cookies. Diese werden nicht von der besuchten Webseite abgelegt, sondern von der Webseite einer Drittpartei, deren Objekte - beispielsweise Werbeeinblendungen - auf der besuchten

Seite erscheinen. Hier handelt es sich um einen einschneidenden Eingriff in die Privatsphäre, da der Nutzer nicht damit rechnen kann, solche Cookies zu erhalten. Wenn eine Werbung auf mehreren anderen Websites erscheint, kann der Nutzer anhand der Spur, welche die Drittanbieter-Cookies hinterlassen, beim Surfen verfolgt werden.
Flash Cookies (local shared objects) verfügen über viel mehr Speicherplatz als die herkömmlichen Cookies. Die Information, die sie enthalten können, ist damit auch viel gewichtiger. Überdies haben diese Cookies die Eigenschaft, dass sie für verschiedene Browser sichtbar sind und nicht nur für denjenigen, der zum Zeitpunkt der Ablage des Cookie auf dem Computer benutzt wurde.
Die letzte Entwicklung schliesslich, die wir bei den Cookies festgestellt haben, ist das Auftreten von Evercookies. Sie haben die Fähigkeit, sich zu vervielfachen und Kopien in verschiedenen Bereichen des PCs anzulegen. Um ein solches Cookie zu deaktivieren, muss man nicht nur das «Original», sondern auch seine sämtlichen Kopien löschen - es können bis zu deren 13 sein. Es braucht nur eine einzige Kopie vergessen zu gehen, damit sich das Cookie automatisch erneut repliziert. Die Cookies auf die übliche Art zu löschen, genügt also nicht, um als Nutzer gegenüber den besuchten Websites wieder eine gewisse Anonymität zu erlangen.
Aufgrund verschiedener Tests wurde festestellt, dass diese Evercookies äusserst schwer zu beseitigen sind. Verschiedene Löschmethoden müssen miteinander kombiniert werden, und es bleiben immer Kopien übrig, die sich nicht auf einfache Weise vernichten lassen. Als Reaktion auf diese neue Technologie sind verschiedene Projekte in Entwicklung, die sich aber bei unseren Tests nicht als zuverlässig erwiesen.
Wie die Entwicklung bei den Cookies zeigt, wird es immer schwieriger, beim Surfen im Internet anonym zu bleiben. Diese in die Computer eingespeisten und schwer löschbaren Informationen geben den Webseiten Aufschluss über die Surfgewohnheiten jedes Nutzers und damit über seine Vorlieben, seine Interessensgebiete und vieles mehr.

4 Datenschutzkonformer Umgang mit den Sozialen Netzwerken

4.1 Zweck dieser Information

Die Bedeutung von Sozialen Netzwerk Anwendungen im Internet ist in den letzten Jahren kontinuierlich gestiegen. Alleine in der Schweiz sind heute 2.48 Mio. Facebook Benutzeraktiv. Anbieter wie Facebook und Co. ziehen nach eigenen Angaben weltweit jeden Monat jeweils weit mehr als 100 Millionen Besucher auf Ihren Webseiten an.

Soziale Netzwerke und die in ihnen abgelegten persönlichen Profile (Daten) haben heute einen wichtigen Stellenwert bekommen. Sie repräsentieren die virtuellen Identitäten der Nutzer im Internet. Hier stellt sich die Frage: wie können soziale Netzwerke und ihre positiven Aspekte sinnvoll genutzt, die eigene Privatsphäre jedoch in ein vertretbares Verhältnis dazu gesetzt werden?

4.2 Risiken für den Anwender

Was passiert, wenn Ihr (zukünftiger) Arbeitgeber Ihre Fotos der letzten feuchtfröhlichen Party sieht? Wofür könnten Betrüger Informationen über Ihre Arbeit oder geplante Urlaube ausnutzen? Diese und andere Fragen sollten Sie sich stellen, bevor Sie ein Profil in einem sozialen Netzwerk anlegen beziehungsweise bevor Sie dort jede Menge Informationen über sich preisgeben.

4.2.1 Offenlegung privater Informationen

In sozialen Netzwerken können Nutzer E-Mail-Adressen, Telefonnummern, Hobbys, Vorlieben und diverse persönliche Informationen angeben. Diese Daten können von Firmen dazu missbraucht werden, die Nutzer gezielt mit Werbung zu bombardieren. Die Voreinstellungen zum Schutz der Privatsphäre sind bei Eröffnung eines Accounts oft nicht ausreichend vorgenommen. Alle Daten sind so automatisch für alle Nutzer des sozialen Netzwerks sichtbar. Auszüge der Profile können teilweise sogar über Suchmaschinen gefunden werden und sind so allen Internetnutzern weltweit zugänglich. Im Bewerbungsprozess nutzen Arbeitgeber soziale Netzwerke, um Informationen überpotentielle Mitarbeiter herauszufinden. Freizügige Fotos oder verfängliche Äusserungen werden da schnell zum k.o.-Kriterium. Auch Vermieter und Versicherungen könnten an den preisgegebenen Hintergrundinformationen interessiert sein. Informationen, Texte und insbesondere Bilder werden häufig von Privatpersonen auch ausserhalb der Netzwerke auf dem eigenen Computer archiviert. So können Daten plötzlich auf anderen Seiten im Internet auftauchen oder für andere Zwecke missbraucht werden –auch nachdem diese vermeintlich aus dem sozialen Netzwerk gelöscht wurden.

4.2.2 Identitätsdiebstahl

Kriminelle versuchen zunehmend, bestehende Nutzer-Accounts zu hacken, um diese Identität für ihre Betrügereien zu nutzen. Oftmals täuschen sie nach Übernahme eines Accounts eine Notsituation vor und bitten die vernetzen Freunde um finanzielle Hilfe. Das über das Nutzerprofil erlesene Wissen kann dazu beitragen, das Vertrauen zu untermauern und Freunde zu täuschen. „Unechte“ Profile werden zunehmend dazu genutzt, Personen zu schaden: Diebe können so zum Beispiel ausspionieren, wann jemand im Urlaub ist und die Wohnung leer steht.

4.2.3 Verbreitung von Schadsoftware

Das Vertrauen der Nutzer in die sozialen Netzwerke ist meist gross. Betrüger haben deshalb eine gewohnte Masche auf diese Plattformen übertragen: Sie verschicken Nachrichten, die einen Link auf manipulierte Webseiten enthalten. Über diese Seiten werden dann die Schadprogramme verbreitet. Ein bekanntes Beispiel hierfür ist der Wurm „Koobface“, der zum Beispiel über Facebook verbreitet wurde. Von zuvor infizierten Konten aus wurden Einladungen an andere Nutzer verschickt, sich ein Video anzusehen. Klickte der Empfänger auf den angegebenen Link, wurde er jedoch auf eine gefälschte Facebook- oder YouTube- Seite geleitet, auf der er zum Download des Flash-Players aufgefordert wurde. Hinter dem angebotenen Download verbarg

sich aber der Wurm, der sich so immer weiter verbreiten konnte. Einige soziale Netzwerke bieten Zusatzanwendungen an, die Nutzer ihrem Profil hinzufügen können. Ein Beispiel hierfür sind Mini-Spiele, die die Nutzer auch vernetzt spielen können. Problematisch ist, dass diese Anwendungen von Drittanbietern stammen, deren Sicherheitsstandards nicht zwangsläufig denen der sozialen Netzwerke entsprechen müssen. Auf diese Weise können – ob beabsichtigt oder ungewollt – Schadprogramme verbreitet werden.

4.2.4 Mobbing

Soziale Netzwerke haben Mobbing auf eine neue Ebene gebracht. Personen können zum Beispiel bewusst aus Freundesgruppen ausgeschlossen oder ihre digitalen Pinnwände mit Beleidigungen bombardiert werden. Dies kann vor allem für Jugendliche zu einer Belastung werden. Mobbing wird strafrechtlich verfolgt. Freundschaften sind in sozialen Netzwerken schneller geschlossen als in der „realen“ Welt. So gelangen Informationen an Personen, die diesen sonst vielleicht nicht anvertraut worden wären. Wer böswillige Absichten hat, kann diese Informationen dafür nutzen, um jemanden bewusst bloss zustellen oder gegen ihn zu intrigieren.
So genannte „Cyberstalker“ können sich auch „unechte“ Profile anlegen, in denen sie sich als eine reelle oder fiktive andere Person ausgeben. So können sie in vollkommener Anonymität andere Personen über das soziale Netzwerk belästigen.

4.3 Verhaltensregeln zum sicheren Umgang mit Sozialen Netzwerken

Millionen Internet-Benutzer knüpfen Kontakte und pflegen Freundschaften über das Internet. Sie legen in Facebook & Co. ein persönliches Profil an, das neben grundlegenden Angaben zu ihrer Person auch Informationen über Hobbys, die Familienverhältnisse oder den beruflichen Werdegang enthalten kann. Das Ziel sozialer Netzwerke ist, sich mit Freunden zu vernetzen und Inhalte zu teilen. Damit sich alle Nutzer in einem sozialen Netzwerk wohl fühlen, ist es wichtig, dass Sie sich an einige Verhaltensregeln - die auch im realen Leben gelten - halten. Die soziale Vernetzung soll Spass machen, und damit es auch so bleibt, ist ein freundlicher und respektvoller Umgang miteinander vorausgesetzt. Mit den folgenden 12 Verhaltensregeln sind Sie gut gerüstet für das soziale Leben im Internet.

1. Seien Sie zurückhaltend mit der Preisgabe persönlicher Informationen!
Nicht alles, was Sie über sich wissen, müssen andere Menschen wissen. Überprüfen Sie kritisch, welche privaten Daten Sie „öffentlich“ machen wollen. Bedenken Sie zum Beispiel, dass immer mehr Arbeitgeber Informationen über Bewerber im Internet recherchieren. Auch Headhunter, Versicherungen oder Vermieter könnten an solchen Hintergrundinformationen interessiert sein.

2. Erkundigen Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Netzwerks!
Mit beidem sollten Sie sich gründlich vertraut machen – und zwar bevor Sie ein Profil anlegen. Nutzen Sie unbedingt die verfügbaren Optionen des sozialen Netzwerks, mit denen die von Ihnen eingestellten Informationen und Bilder nur eingeschränkt „sichtbar“ sind: Sollen nur Ihre Freunde Zugriff darauf haben oder auch die Freunde Ihrer Freunde oder alle Nutzer?

3. Seien Sie wählerisch bei Kontaktanfragen – Kriminelle „sammeln“ Freunde, um Personen zu schaden!
Bei Personen, die Sie nicht aus der „realen“ Welt kennen, sollten Sie kritisch prüfen, ob Sie diese in Ihre Freundesliste aufnehmen wollen. Der oder die Unbekannte könnte auch böswillige Absichten haben. Kriminelle könnten zum Beispiel ausspionieren, wann Ihre Wohnung leer steht. „Unechte Profile“ werden nachweislich dazu genutzt, Personen zu schaden – sei es aus Rache, Habgier oder anderen Beweggründen.

4. Melden Sie „Cyberstalker“, die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren!
Dafür können Sie sich meistens direkt an die Betreiber des jeweiligen sozialen Netzwerkes wenden. Diese können der Sache nachgehen und gegebenenfalls das unseriöse Profil löschen. In besonderen Fällen sollten Sie auch die Polizei für eine Strafverfolgung informieren.

5. Verwenden Sie für jede Internetanwendung, insbesondere auch wenn Sie in verschiedenen sozialen Netzwerken angemeldet sind, ein unterschiedliches und sicheres Passwort!
Seien Sie sich aber auch darüber bewusst, dass Ihre Daten auf fremden Rechnern gespeichert sind. Das heisst die Sicherheit Ihrer Daten hängt nicht nur von Ihnen ab, sondern auch von den Betreibern des sozialen Netzwerks: wird deren Server gehackt, sind Ihre Daten nicht mehr sicher. Wenn Missbrauch bekannt wird, informieren Sie auch Ihre Freunde.

6. Geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis!
Berufliche Informationen haben in sozialen Netzwerken nichts verloren. Auch Wirtschaftsspione haben soziale Netzwerke für sich entdeckt und versuchen dort, wertvolle Informationen abzuschöpfen. Das kann Ihre Firma Geld und Sie den Job kosten.

7. Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen!
Keine Leistung ohne Preis: Die Eintrittskarte in soziale Netzwerke kostet Sie die Preisgabe von Informationen. Viele Firmen sind bereit, für diese Daten Geld zu bezahlen, um gezielt Werbung verschicken zu können. Geben Sie den sozialen Netzwerken die Rechte an Ihren Bildern, können diese theoretisch von den Betreibern weiterverkauft werden. Prüfen Sie auch, ob das gewährte Nutzungsrecht womöglich bestehen bleibt, wenn Sie Ihr Profil löschen.

8. Wenn Sie „zweifelhafte“ Anfragen von Bekannten erhalten, erkundigen Sie sich ausserhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachricht!
Identitätsdiebstahl ist ein Risiko des digitalen Zeitalters. Eine fremde Person kann mit Hilfe eines gehackten Accounts, eine fremde Identität übernehmen und deren Freunde täuschen. Betrüger können zum Beispiel Nachrichten verschicken, in denen sie eine Notsituation beschreiben und um finanzielle Hilfe bitten. Mit Hilfe des angelesenen Wissens über die gestohlene Identität kann dabei die Vertrauenswürdigkeit untermauert werden.

9. Klicken Sie nicht wahllos auf Links – Soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben! Auf einen Link ist schnell geklickt. Aber Vorsicht: die Zieladresse könnte eine gefälschte Startseite eines sozialen Netzwerkes sein. Geben Sie dort Ihren Benutzernamen und Kennwort ein, werden die Daten direkt an die Betrüger weitergeleitet. Besonders beliebt sind bei solchen Attacken so genannte Kurz-URLs, bei denen der Nutzer die eigentliche Zieladresse nicht erkennen kann.

10. Sprechen Sie mit Ihren Kindern über deren Aktivitäten in sozialen Netzwerken und klären Sie sie über die Gefahren auf!
Viele Kinder und Jugendliche sind sich oft nicht bewusst, welche Gefahren in sozialen Netzwerken lauern – Spass geht ihnen häufig vor Sicherheit. Die Stärkung der „Medienkompetenz“ ist eine neue Aufgabe, die Eltern in der Erziehung übernehmen müssen. Aber auch mit anderen Familienangehörigen und Freunden sollten Sie sich über Risiken und Bedenken austauschen.

11. Arbeitgeber, die die Verwendung von Social Networks wie Facebook etc. im Unternehmen erlauben, sollten eine sogenannte Social Media Weisung erstellen und die Mitarbeitenden mit dem Umgang entsprechend sensibilisieren. Die Social Media Weisung soll als Ergänzung zum Arbeitsvertrag von jedem Mitarbeiter unterschrieben werden.

12. Benutzen Sie Facebook auf mobilen Geräten, können die Facebook-Benutzer ihren aktuellen Standort erkennen. So wissen mögliche Einbrecher, dass Sie im Moment nicht zu Hause sind. Achten Sie darauf, dass Sie diese Funktion deaktivieren oder nur gezielt einsetzen.

5 Terravis, das Auskunftsportal für Grundbuch-Kunden

5.1 Ausgangslage

Das Projekt eGRIS hat zum Ziel, eine Infrastruktur zu etablieren, die eine schweizweite Abfrage von Grundbuchdaten und die elektronische Abwicklung des Geschäftsverkehrs mit den kantonalen Grundbüchern ermöglicht. Im Kanton Thurgau ist «Terravis» am 1. Sept. 2011 produktiv aufgeschaltet worden. Es geht darum, das schweizweit geplante Auskunftsportal in der praktischen Anwendung zu überprüfen.

5.2 Gesetzliche Rahmenbedingungen

Massgabe für die Führung des Grundbuches mittels EDV bilden Art. 942 Abs. 3 in Verbindung mit Art. 949a ZGB. Das Grundbuch kann und wird in vielen Kantonen mittels Informatik geführt. In der Grundbuchverordnung (GBV) werden in den Art. 111 ff. die damit verbundenen Auflagen konkretisiert. Art. 111l GBV beschäftigt sich mit der Auskunft und Einsichtnahme in Grundbuchdaten. Die Kantone dürfen die Daten des Hauptbuches über die jede Person ohne das Glaubhaftmachen eines Interesses Auskunft verlangen kann, in öffentlichen Datennetzen zur Verfügung stellen. Sie müssen sicherstellen, dass die Daten nur grundstücksbezogen abgerufen werden können und dass die Auskunftssysteme vor Serienabfragen geschützt sind. In Art. 111m GBV werden die Personen und Behörden aufgeführt, welche über Abrufverfahren Zugriff auf die Grundbuchdaten haben können.

Die Kantone wurden gesetzlich nicht verpflichtet, die Grundbuchdaten in öffentlichen Netzen zur Verfügung zu halten. Die Definition «öffentliche Datennetze» lässt Spielraum. Die Tatsache, dass die Revision auf das Jahr 2005 zurückgeht, lässt den Schluss zu, dass eine internetmässige Aufschaltung möglich sein soll. Ab welcher Anfrage von einer Serie ausgegangen werden muss, wird nicht umschrieben. Bis zu vier Abfragen werden wahrscheinlich nicht unter diesen Begriff fallen. Ansatzweise wird also der Versuch unternommen, einen kommerziellen Nutzen oder die reine Neugier dem Schutz der Persönlichkeit unterzuordnen.

Die in Revision begriffene Grundbuchverordnung weitet die Zugriffsmöglichkeit und damit die Öffentlichkeit massiv aus. Im Gegensatz zu heute sollen sämtliche Anmerkungen bekannt gegeben werden dürfen (vgl. Art. 106 Abs. 1 lit. c Ziff. 1– 4 GBV und Art. 29 Abs. 1 E-GBV). Somit werden beispielsweise Grundbuchsperren im Rahmen einer Scheidung öffentlich. Art. 30 Abs. 1 E-GBV verpflichtet die Kantone, den Zugriff auf Daten des Hauptbuches öffentlich zugänglich zu machen. Die vorgesehenen Bestimmungen bauen auf den derzeit gültigen Artikeln auf und erweitern die Zugriffsmöglichkeiten.

5.3 Beurteilung

Art. 13 Abs. 1 BV garantiert jeder Person ihren Anspruch auf Achtung ihres Privat- und Familienlebens sowie ihrer Wohnung. Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 BV). Es bedarf somit bei jeder Gesetzesrevision mit datenschutzrechtlicher Relevanz einer Interessenabwägung. Mit Bezug auf die bestehende und geplante internetmässige Aufbereitung von Grundbuch-Basisdaten stellt sich somit die Frage, ob das öffentliche Interesse auf eine weltweite Veröffentlichung höher zu gewichten ist, als der von der Verfassung garantierte Schutz der Privatsphäre.

In diesem Zusammenhang interessiert insbesondere die Frage, worin das öffentliche Interesse einer Veröffentlichung überhaupt besteht. Die Allgemeinheit zieht grundsätzlich keinen Nutzen aus der Bekanntgabe der persönlichen Grundbuchdaten. Es bedarf vielmehr konkreter Gründe, die eine Person veranlassen, die Eigentümerschaft eines Grundstückes zu wissen; zu denken ist an einen Kauf, die Einräumung von dinglichen Rechten oder etwa die Hypothezierung einer Liegenschaft. Für im Grundstückgeschäft tätige Personen und Unternehmen ist ohnehin eine Spezialnorm vorgesehen.
Es bleibt deshalb kaum Raum für die allgemeine Zugänglichmachung von Grundbuchdaten. Demgegenüber steht das Interesse des Einzelnen auf Kontrolle des Bearbeitungszweckes, auf die Vermeidung von Rückschlüssen auf die persönlichen Verhältnisse, auf den Schutz vor Belästigung, Bedrohung oder Kommerzialisierung der Daten. Und schliesslich darf die Möglichkeit der Erarbeitung eines Persönlichkeitsprofils unter Einbezug von Google, Google Map, Street View etc. nicht unterschätzt werden.
Im Datenschutzrecht wird dem Prinzip der Verhältnismässigkeit eine nicht unerhebliche Bedeutung beigemessen. Es dürfen somit nur diejenigen Daten voraussetzungslos veröffentlicht werden, welche für die Allgemeinheit von Interesse sind und ihr einen Zusatznutzen bringen. Auch unter diesem Aspekt lässt sich kein Grund finden, der für eine weltweite Veröffentlichung der Grundbuchdaten spricht. Es bleibt vorerst abzuwarten, ob Art. 111l GBV und Art. 30 E-GBV einer allfälligen verfassungsmässigen Überprüfung standhalten würden.

5.4 eGRIS

Die Nutzung der modernen Kommunikations- und Speichermittel hat im Grundbuchwesen schon vor Jahren Einzug gehalten. Mit dem Produkt «Auskunftsportal Thurgau» soll Praxiserfahrung gesammelt werden. Dabei basiert die Applikation auf der revidierten Grundbuchverordnung, welche voraussichtlich am 1. Januar 2012 in Kraft treten soll. Unter den Beteiligten werden neben den öffentlichen Daten Vormerkungen, Grundpfandrechte, technische Bemerkungen und Hinweise auf hängige Geschäfte ausgetauscht. Gerade darin liegt die grosse Problematik. Gemäss Art. 31 E-GBV in Verbindung mit Art. 32 Abs. 1 E-GBV sollen beispielsweise Banken, Pensionskassen und Versicherungen mittels eines Abrufverfahrens Zugang zu den erweiterten Daten erhalten. Einschränkungen des Zugriffs sind gesetzestechnisch nicht vorgesehen. Entgegen des allgemein anerkannten Grundsatzes, wonach Listenauskünfte und gleichermassen natürlich Serienabfragen für kommerzielle Zwecke nicht statthaft sind, werden vorliegend im Wettbewerb stehende Unternehmen am Datenaustausch beteiligt.
Aus datenschutzrechtlicher Sicht sind flankierende Massnahmen zwingend erforderlich. Dazu gehört neben der vorgesehenen Protokollierung ein Informationsfluss an den Eigentümer. Mit dem Einbezug der Betroffenen wird vor allem Transparenz geschaffen und der Eigentümerschaft die Möglichkeit geboten, das verfassungsmässige Recht auf missbräuchliche Verwendung von persönlichen Daten gegebenenfalls durchzusetzen.

6 Weitere datenschutzrelevante Projekte

6.1 Brustkrebsscreening / Krebsregister

6.2 Projekt „Guter Start ins Kinderleben“

6.3 GIS

6.3.1 Denkmaldatenbank

6.3.2 ThurGis Orthofotos

7 Aufsichtsstelle

7.1 Statistik der Tätigkeiten

Statistik Tätigkeiten
DSB 2011

Wer	Anfragen	Beratungen	Kontrollen	Vernehmlassungen	Referate	Weiterbildung
Kant. Verwaltung	21	15		4		
öff. Rechtl. Anstalten	3					
Gemeinden	15	10				
Privatpersonen	25	15				
Andere					2	6
Total	**64**	**40**		**4**	**2**	**6**