Datenschutz – Eine Querschnittsmaterie

Michael Sonntag

Johannes Kepler Universität Linz
Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)
Altenbergerstr. 69, A-4040 Linz, Österreich
sonntag@fim.uni-linz.ac.at

Datenschutz ist zwar als Querschnittsmaterie bekannt, dies wird aber typischerweise so verstanden, dass er in allen Fachbereichen erforderlich ist, d.h. unabhängig von der konkreten Anwendung überall dort, wo personenbezogene Daten auftreten. Doch auch direkt im Softwareentwicklungsprozess kann Datenschutz als Querschnittsmaterie angesehen werden: In allen Phasen der Softwareerstellung sind spezifische Anforderungen bzw. Einschränkungen durch den Datenschutz zu berücksichtigen. Einige davon werden beispielhaft erläutert und daraus abschließend argumentiert, dass jede universitäre Ausbildung für Informatiker auch gewisse rechtliche Grundelemente beinhalten sollte.

1 Einführung

Datenschutz (DS) ist ein derzeit stark diskutierter rechtlicher Aspekte, insbesondere im Hinblick auf Sicherheit und Strafverfolgung: Von Urheberrechtsverletzungen bis hin zu Terrorismus. Aufgrund vielfältiger gesetzlicher Vorgaben ist daher eine extensive Berücksichtigung schon bei der Softwareerstellung erforderlich und wird immer wichtiger. In welchen Phasen dies jedoch konkret Modifikationen bzw. Ergänzungen erfordert, erscheint eher unklar. Relativ eindeutig ist die Berücksichtigung bei der Anforderungsanalyse, zB bei dem Erfordernis der Einholung von Zustimmungserklärungen Betroffener. Doch auch verschiedene andere Stufen des Softwareentwicklungsprozesses sind betroffen.

2 DS in den Entwurfsphasen

Die folgenden Erörterungen basieren auf dem Wasserfallmodell. Auch wenn es in der Praxis kaum mehr eingesetzt wird, zeigt es doch die verschiedenen Stufen, die auch in anderen Vorgehensmodellen wie zB dem Spiralmodell erforderlich sind, in großer Klarheit.

2.1 Anforderungsanalyse

Ein Grundprinzip des DS ist das Minimalitätsprinzip: Es dürfen nur Daten erhoben werden, die für den angestrebten Zweck erforderlich sind (Art. 6 Abs 1 lit c [DS-RL]). Es ist daher erforderlich, diesen Zweck schon zu Beginn exakt zu spezifizieren, insbesondere da spätere Datenübertragungen oder Änderungen des Verwendungszwecks besondere rechtliche Anforderungen erfüllen müssen: Derartige Übermittlungen benötigen zB eine Zustimmung, für welche die Empfängerkreise anzugeben sind. Da generelle Zustimmung verboten ist, müssen die Empfänger schon bei der Erhebung definiert werden, soll nicht später eine neuerliche Einwilligung eingeholt werden müssen.

Nicht vergessen werden darf, dass auch Hilfs-Prozesse erforderlich sind: Betroffene können der Verwendung ihrer Daten großteils jederzeit widersprechen (§§ 8 Abs 1 Z 2, 28 [DSG]), sodass auch entsprechende Löschverfahren vorzusehen sind. In bestimmten Fällen ist zusätzlich die Hinzufügung eines Bestreitungsvermerks vorzusehen (§ 27 Abs 7 DSG). In diese Phase gehören auch die Integration von Robinsonlisten bzw. Verfahren zur regelmäßigen Aktualisierung bzw. Korrektur personenbezogener Daten.

2.2 Systemdesign

Der Entwurf der Systemarchitektur muss berücksichtigen, wo und wie personenbezogene Daten gespeichert werden, zB in pseudonymisierter Form mit separater Datenbank zur Herstellung des Personenbezugs nur in den erforderlichen Fällen, oder auf Server bzw. Client.
In der Praxis unbekannter ist die Bereitstellung definierter Schnittstellen, um gesetzlichen Anforderungen nachkommen zu können. Dies beinhaltet zukünftig, sofern anwendbar, die verpflichtende Vorratsdatenspeicherung. Weiters ist etwa das Löschen von Daten während eines laufenden Verfahrens, aber auch für vier Monate nach einem Auskunftsbegehren, verboten (§ 26 Abs 7 DSG), weshalb derartige laufende Verfahren zu speichern sind.

Entsprechend dem von den Daten ausgehenden Risiko ist eine Protokollierung der Verarbeitungsschritte vorzusehen (§ 14 Abs 2 Z 7 DSG). Solche Protokolle dürfen jedoch nicht (auch) anderen Zwecke dienen: So ist es beispielsweise verboten, den Zeitpunkt der manuellen Eingabe bei elektronischer Arbeitszeiterfassung zur Kontrolle der Eingabedaten zu verwenden [Brodil].

2.3 Implementation

Bei der Implementierung sind alle erforderlichen Sicherheitsvorkehrungen (§ 14 DSG) umzusetzen, ebenso wie zB die Protokollierung. Doch auch hier stellen sich Detailfragen. Wie müssen Informationspflichten erfüllt werden (Ort, Verlinkung, Datenformat, optischer Her-

vorhebungen etc.)? Hier sind insbesondere die Regelungen für AGB's maßgeblich, ergänzt um datenschutzrechtliche Sondervorschriften. Darf etwa ein Webshop bei der Zustimmungserklärung zur Datenverwendung das Kästchen bereits angehakt darstellen oder muss der Besucher dies selbst vornehmen? In Deutschland muss der Benutzer dies selbst tun (§ 4 Abs 2 Z 1 [TDDSG]), in Österreich hingegen nicht, wo auch eine konkludente Zustimmung möglich und ausreichend ist.

2.4 Test

Auch in der Testphase ist der DS zu berücksichtigen. Eine beliebte Vorgehensweise bei Tests ist es, Echtdaten zu verwenden. Problematisch ist hierbei der Einsatz personenbezogener Daten, welche dadurch Entwicklern zugänglich werden, die eigentlich keinen Zugriff darauf besitzen dürften. Weiters ist in der Testphase ja noch nicht festgestellt, ob alle Sicherheitsvorkehrungen etc. tatsächlich funktionieren, bzw. werden diese zeitweise sogar absichtlich ausgeschaltet. Auch erfolgen Tests nicht unbedingt in einer abgeschotteten Umgebung sondern bei den Entwicklern. In Frage kommt daher rechtlich gesehen ausschließlich der Einsatz anonymisierter oder künstlicher Daten, zB randomisierte oder durch Generatoren erzeugte Phantasienamen/-adressen.

2.5 Einführung

Während der Einführung hat, falls erforderlich, die Anmeldung bei Datenverarbeitungsregister zu erfolgen. Je nach Datenverarbeitung ist ev. eine Vorabkontrolle erforderlich, sodass die tatsächliche Inbetriebnahme erst nach Erteilung der Genehmigung erfolgen darf.

Dieser Phase kann weiters das Anlegen von Benutzerkonten zugerechnet werden. Hierbei sind Anwender auf die Datenschutzvorschriften (insb. § 15 DSG - Datengeheimnis) hinzuweisen und dies zu protokollieren, was auch vom Programm selbst erledigt werden kann, zB durch Anzeige eines entsprechenden Textes und obligatorischem Klicken eines Akzeptanz-Buttons, sodass ein späterer Beweis darüber möglich ist.

2.6 Nutzung

Während der Nutzung sind Datenschutz- und Datensicherheitsvorschriften einzuhalten. Hinsichtlich Softwareerstellung ergeben sich wenig besonderen Aspekte.

Basiert die Lizenzierung von Software auf einer Abrechung nach tatsächlicher Verwendung so ist zu berücksichtigen, dass die Nutzungsdaten keinen Rückschluss auf die bearbeitenden Personen zulassen sollten.

2.7 Wartung

Hierbei gilt ähnliches wie bei Tests: "Echte" Daten dürfen Entwicklern nicht zugänglich gemacht werden. In dieser Phase bestehen jedoch bedeutende Einschränkungen: Theoretisch wäre es nicht einmal erlaubt, Datensätze die Fehler verursachen oder die als Beispiele für Erweiterungen dienen, an Entwickler weiterzuleiten. Ohne die konkreten Daten ist jedoch der Fehler vielfach nicht einzugrenzen. Hier kann daher mit einem überwiegenden berechtigten Interesse des Verwenders argumentiert werden, sodass derartige Übermittlungen einzelner Datensätze rechtmäßig sind. Besonders dann ist jedoch das Datengeheimnis zu wahren, d.h. die Daten dürfen von den Entwicklern nicht weitergegeben bzw. für sonstige Zwecke verwendet werden.

3 Zusammenfassung

Datenschutz betrifft also keineswegs ausschließlich die Entwurfsphase, sondern muss kontinuierlich und während des gesamten Softwareentwicklungszyklus beachtet werden. Sie ähnelt damit der Sicherheit, welche ebenfalls in allen Teilen der Entwicklung zu berücksichtigen ist. Gemeinsam ist beiden, dass sie in der Praxis oft anderweitig "implementiert" werden: Als Gedanke im Nachhinein, was zu vielen Problemen führt, wenn sie einem (fast) fertigen Produkt hinzugefügt werden sollen. Genauso wie ein Verschlüsselungsalgorithmus recht einfach auszutauschen ist, können auch Kästchen zum Anhaken leicht umgestellt werden. Demgegenüber ist jedoch ein unsicheres Protokoll später nur schwer abzusichern oder auf pseudonymisierte Datenübertragung umzustellen.

Deshalb sollte jedes Studium der Informatik grundlegende Kenntnisse über den DS vermitteln, nicht nur im Bereich der Wirtschaftsinformatik, sondern ebenso bei rein "technischen" Informatik-Studiengängen, um das Bewusstsein für und die inhaltlichen Grundzüge von rechtlichen Rahmenbedingungen zu schaffen. Genauso sollten Grundkenntnisse des Urheberrechts zur Basisausbildung für Informatiker gehören. Daher enthält der derzeit in Ausarbeitung befindliche neue Studienplan für Informatik in Linz eine einstündige Lehrveranstaltung über rechtliche Grundlagen. Für diese ist schon jetzt ein Lehrbuch ([EBR]) erschienen, in welchem ganz besonders der Datenschutz näher erläutert wird.

4 Literatur

[Brodil] Brodil: Zeiterfassung ohne Zeiterfassung? ecolex 2005, 459 zur Entscheidung DSK 16. 11. 2004, K 120.951/0009-DSK/2004

[DSG] Österreich: Datenschutzgesetz 2000 - DSG 2000, BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 13/2005

[DS-RL] Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. L 281/31 vom 23.11.1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31995L0046:DE:HTML

[EBR] Michael Sonntag: E-Business Recht - Eine Einführung für Informatiker. Linz: Universitätsverlag Rudolf Trauner 2006. Details und Bestellmöglichkeit: http://elearning.fim.uni-linz.ac.at/cms/wl_ebiz.phtml

[TDDSG] Deutschland: Gesetz über den Datenschutz bei Telediensten, BGBl I 1997, 1870 idF BGBl I 2001, 3721