MEDIEN-ETHIK

HOCHSCHULE DER MEDIEN STUTTGART

ESSAY

ETHIK-CODEX FÜR EIN FIKTIVES UNTERNEHMEN

Verfasser:	Benjamin Zaiser
E-Mail:	bz003@hdm-stuttgart.de
Studiengang:	Computer Science and Media
Semester:	3
Datum:	12. Juni 2009

AUFGABENSTELLUNG:

Für ein fiktives Unternehmen soll ein Ethik-Codex ausgearbeitet werden. In diesem Dokument wird dabei der Abschnitt im Umgang mit personenbeziehbaren Daten behandelt.

Es sollen Normen ausgearbeitet und begründet werden, die dem Umgang mit personenbeziehbaren Daten zugrunde liegen.

NORMEN FÜR DEN UMGANG MIT PERSONENBEZOGENEN DATEN

ALLGEMEIN

(1) Bei der Verarbeitung personenbezogener Daten müssen die gesetzlichen Bestimmungen des Bundes-Datenschutz Gesetz eingehalten werden.

UMGANG MIT DATEN VON MITARBEITER

(2) Jeder Mitarbeiter stimmt beim Arbeitsvertrag zu, den Internetzugang am Arbeitsplatz nur zu beruflichen Zwecken zu verwenden. Der Arbeitgeber hat das Recht die aufgerufenen Webseiten / Dienste jederzeit stichprobenartig zu überwachen und entsprechende Maßnahmen einleiten.

UMGANG MIT DATEN VON KUNDEN:

(3) Grundsätzlich werden nur die Daten gespeichert, die auch wirklich benötigt werden (z.B. nur Geburtsjahr, anstatt des gesamten Geburtsdatums).

(4) Die Kundendaten unterliegen einem Zugriffsprotokoll, so dass jederzeit nachgewiesen werden kann, wer wann welche Daten verwendet oder bearbeitet hat.

DATENSPEICHERUNG

(5) Die Daten werden ausschließlich an *einem* zentralen Ort gespeichert. Dies wird auch nach außen hin kommuniziert, um eine möglichst hohe Transparenz zu erreichen.

(6) Mitarbeiter dürfen die Daten nicht vervielfältigen oder kopieren (z.B. Download auf lokale Festplatte). Die Daten dürfen nur an einem zentralen Ort abliegen und dürfen auch nur dort bearbeitet werden.

(7) Den Zutritt zu den Datenverarbeitungsanlagen darf nur authentifizierten Personen gewährt werden (Zutrittskontrolle).

(8) Die Anlagen dürfen nur von autorisierten Personen genutzt werden (Zugangskontrolle)

(9) Autorisierte Personen dürfen nur Zugang zu Daten erhalten, für die sie eine Zugriffsberechtigung besitzen. Nach der Verarbeitung, Nutzung und Speicherung dürfen die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (wie z.B. durch den Browser-Cache oder ähnliches).

(10) Personen, deren Daten gespeichert wurden, können jederzeit die Löschung der Daten aus der Datenbank des Unternehmens verlangen.

DATENÜBERMITTLUNG / -WEITERGABE

(11) Bei der Übermittlung der Daten über das Internet wird eine den aktuellen Sicherheitsstandards entsprechende abgesicherte Verbindung aufgebaut. So kann ausgeschlossen werden, dass die Daten von einem Dritten abgefangen und unter Umständen missbraucht werden können.

(12) Bei einer Veröffentlichung von Daten (Name, Adresse, Bilder, etc.) auf unserer Website muss eine Freigabe von der entsprechenden Person vorliegen.

(13) Bei der Weitergabe von personenbezogenen Daten an Dritte muss zuvor die Einverständniserklärung der betreffenden Person angefordert werden.

Erstellt unter Verwendung folgender Quellen (meist sinngemäß übernommen, siehe Literaturverzeichnis):
(BITKOM (Bundesverband Informationswirtschaft 2008), (Bistümer 1991), (Initiative 2002), (e.V. 2003)

BEGRÜNDUNG ZUR AUSWAHL DER NORMEN

ZU (1):

Grundsätzlich muss das Unternehmen die Gesetze, die im Bundesdatenschutzgesetz (BDSG) enthalten sind, respektieren und einhalten. Das BDSG in Deutschland beinhaltet bereits eine Vielzahl an Normen. Deswegen wurden bei der Ausarbeitung des Kodex einige besonders wichtige Normen explizit erwähnt, obwohl diese bereits im BDSG enthalten sind.

ZU (2):

Aus der Sicht des Unternehmens ist es nicht vertretbar, dass Mitarbeiter Ressourcen (Internetzugang, Arbeitszeit, …) verschwenden, um private Angelegenheiten zu erledigen. Laut des OVG Mecklenburg-Vorpommern, Beschluss vom 21.12.2000, 2 M 64/00; (e.V. 2003) hat das Unternehmen das Recht, die Mitarbeiter hierbei zu überwachen und entsprechend zu verweisen. Die Daten dürfen jedoch nicht auf Vorrat gespeichert werden, was in diesem Fall auch nicht notwendig ist.

ZU (3):

Um einen möglichen Missbrauch der Daten zu minimieren und die Akzeptanz der Kunden, gewisse Daten angeben zu müssen zu maximieren, sollte stets so wenig wie möglich und nur so viel wie nötig gespeichert werden. Wird z.B. im Unternehmen nur das Geburtsjahr benötigt, so sollten die zusätzlichen Daten wie Geburtstag und Geburtsmonat vom Kunden nicht angegeben werden müssen.

ZU (4):

Durch ein Zugriffsprotokoll kann jederzeit überprüft werden, welcher Mitarbeiter welche Daten wofür verwendet hat. So entsteht ein „Lebenslauf“ der gespeicherten Daten, der später auch bei rechtlichen Fragen hilfreich sein kann. Wenn z.B. der Besitzer der Daten rechtliche Schritte einleitet, weil diese unter Umständen missbraucht wurden, ist es mithilfe des Protokolls möglich, genau zu überprüfen, ob die Beschuldigung auch rechtmäßig ist. Auch für den Besitzer der Daten und für das Unternehmen ist es von Vorteil, mithilfe des Zugriffsprotokolls detailliert die Verwendung der Daten nachweisen zu können.

ZU (5):

Nur wenn alle sensiblen Daten an einem Ort gespeichert werden, ist eine Kontrolle und Überwachung der Daten möglich. Würden die Daten an vielen verschiedenen Orten

gespeichert, so könnte nur sehr schlecht bzw. mit sehr hohem Aufwand z.B. ein Zugriffsprotokoll erstellt werden. Falls ein Kunde die Löschung seiner Daten beantragt, kann nur durch den einen zentralen Speicherort gewährleistet werden, dass die Daten auch im gesamten Unternehmen gelöscht werden.

Zu (6):

Damit Punkt (5) auch gewährleistet werden kann, dürfen die Daten von z.B. Mitarbeitern nicht kopiert und an weiteren Orten gespeichert werden.

Zu (7) / (8):

Es muss gewährleistet werden, dass der physikalische Zutritt zum Rechenzentrum, bzw. dem Speicherort der Daten, sowie der „virtuelle" Zugriff auf die Daten nur Personen erlaubt wird, die auch das entsprechende Recht dazu haben. Nur so wird sichergestellt, dass die Zugriffs-Überwachung nicht umgangen werden kann und die Daten ohne entsprechenden Eintrag im Zugriffsprotokoll verändert oder kopiert werden.

Zu (9):

Besitzt z.B. ein Mitarbeiter das Recht, auf bestimmte Daten zugreifen zu dürfen, so muss das System gewährleisten, dass die Person auch wirklich nur auf die Daten zugreifen kann, für die sie berechtigt wurde. Ein Zugriff auf die restlichen Daten muss verhindert werden. Nach der Bearbeitung müssen alle temporären Daten auf dem lokalen Rechner wieder gelöscht werden, um einem möglichen Missbrauch vorzubeugen.

Zu (10):

Grundsätzlich sollte der Kunde das Recht haben, die Löschung seiner Daten zu beantragen. Da dies ein sehr wichtiger Punkt ist, wird dieser hier nochmals explizit aufgeführt, obwohl er bereits im BDSG verankert ist. Durch die Möglichkeit, die Daten wieder zu löschen, kann es dem Besitzer ermöglicht werden, seine „Weste wieder rein zu waschen". Insbesondere z.B. bei unerwünschten Bildern, die ein Personalberater nicht sehen sollte, wenn es um die Evaluation einer Bewerbung der entsprechenden Person handelt ist die Möglichkeit, Daten zu löschen besonders sinnvoll. Ein Spruch besagt: „Das Internet vergisst nie etwas". Um diesem Problem zu entgehen ist zusätzlich auch Punkt 12 von besonderer Bedeutung.

Zu (11):

Bei der Übermittlung der Daten über das Internet könnte theoretisch ein Dritter die Übertragung abfangen und die Daten weiterverwenden oder sogar manipulieren und an den Empfänger weitersenden. Um dies zu verhindern ist es wichtig, dass eine gesicherte Verbindung zwischen Sender und Empfänger etabliert wird, um die Authentizität der Daten zu sichern und das Abhören von Dritten zu verhindern.

Zu (12) / (13):

Sobald Daten auf einer öffentlich zugänglichen Internetseite bereitgestellt werden, kann der Gebrauch dieser Daten nicht mehr kontrolliert werden. Außerdem können die Daten von Dritten kopiert und gespeichert werden (wie z.B. Google Cache, Archive.org, etc.). Es ist deshalb sehr wichtig, dass bei einer Veröffentlichung auf der Internetseite, der Besitzer der Daten darüber informiert wird und er seine Einwilligung geben muss.

Abschließende Anmerkung:

Ein Ethik-Kodex kann niemals von einem einzelnen Mitarbeiter der Firma (wie es in der Aufgabenstellung gefordert wird) erstellt werden. Zunächst muss der Impuls für die Ausarbeitung eines Kodex von der Unternehmensführung kommen, da diese den Kodex vorleben und selbstverständlich auch einhalten muss. Des Weiteren müssen alle Stakeholder (Mitarbeiter, Kunden, etc.) in die Ausarbeitung des Kodex mit einbezogen werden. Dies dient zur Identifikation der Stakeholder mit dem Kodex und nur so kann später auch gewährleistet werden, dass die aufgestellten Normen akzeptiert und respektiert werden (siehe auch (Strobel 2001).

LITERATURVERZEICHNIS

Bistümer, Der Diözesandatenschutzbeauftragte der norddeutschen. *Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnarbrück.* 1991.

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.). *Mustervertragsanlage zur Auftragsdatenverarbeitung (Version 2.1).* 2008.

e.V., FoeBuD. *Recherche zum Arbeitnehmerdatenschutz.* Bielefeld, 2003.

Initiative, eHealth Ethics. *eHealth Ethik-Kodex.* 2002.

Strobel, Frank. *Was bringt ein unternehmensweiter Ethik-Kodex?* Der Schweizer Treuhänder 5/01, 2001.