

Datenschutz als Kommunikationsauftrag

Ansgar Heitkamp | ansgar.heitkamp@uv.hu-berlin.de

„Müssen wir dazu noch den Datenschutzbeauftragten befragen?“ Im schlechtesten Fall erntet diese Frage den gleichen Gesichtsausdruck wie ein Biss in eine Zitrone. Die Bedeutung ist leicht zu erraten: „Ja, wir müssten eigentlich, aber ... geht es nicht vielleicht auch irgendwie ... anders?“

Nein. Es geht nicht.

Sobald personenbezogene Daten per IT verarbeitet werden, greifen die Regelungen des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder. Angesichts der zunehmenden Verknüpfung und Verknüpfbarkeit von Daten kommt dem Merkmal „personenbezogen“ immer weniger einschränkender Charakter zu. Daten gelten bereits dann als personenbezogen, wenn sie Informationen über bestimmbare Personen darstellen. Es reicht also, wenn die Person für Dritte mit nicht unverhältnismäßig großem Aufwand identifizierbar ist.

In Zeiten von Google, yasni und 123people ist dies schnell gegeben. Innerhalb eines Informationsverbundes, wie einer Universität, gilt dies erst recht. Die vor knapp 30 Jahren noch kühn klingende Prognose im Volkszählungsurteil des BVerfG,¹ dass es keine „belanglosen“ Daten mehr gebe, sorgt heute für keine Verwunderung mehr. Teils liest man bereits die Überlegung, auf das Merkmal des Personenbezuges ganz zu verzichten.²

Obwohl der Großteil von IT-Projekten datenschutzrelevante Inhalte betrifft, ist es ein offenes Geheimnis, dass vor Einbindung des behördlichen Datenschutzbeauftragten (behDSB) für einige Verantwortliche nach wie vor eine Hemmschwelle zu überwinden ist. Die Befürchtungen sind vielfältig: Realisierungsdruck, Zeitverzögerung, Kostenexplosion wegen Änderungserfordernissen oder gar die Feststellung, das Vorhaben sei mit dem Datenschutz nicht vereinbar.

Datenschutz als Blackbox?

Das Beispiel oben zeigt ein klassisches Problem in der Zusammenarbeit mit dem behDSB: Das Projekt ist nahezu fertig, der Datenschutzbeauftragte muss „nur“ noch zustimmen. Dabei werden Einbeziehung wie auch Inhalt der Prüfung des behDSB als Blackbox wahrgenommen.

Tatsächlich besteht bei einer solchen Ausgangslage die Gefahr, dass im Projekt neben vielen inhaltlichen Überlegungen und großem Engagement auch bereits diverse datenschutzrechtliche Stolpersteine implementiert sind; die Befürchtungen gegenüber der Einbindung des behDSB werden so zur selbst erfüllenden Prophezeiung. Im Folgenden sollen besonders praxisrelevante Aspekte einer Datenschutzprüfung dargestellt und hieraus Möglichkeiten zur Handhabung abgeleitet werden. Im Zentrum steht dabei die regelmäßige und möglichst frühzeitige Kommunikation und Verständigung zwischen behDSB und den Verantwortlichen eines IT-Projekts

Eine zu späte Überprüfung datenschutzrechtlicher Aspekte eines IT-Vorhabens führt leicht zu Komplikationen oder Verzögerungen bei der Projektrealisierung. Ausgehend von einzelnen Punkten einer datenschutzrechtlichen Prüfung spricht sich der Artikel für einen frühzeitigen Informationsaustausch zwischen Datenschutzbeauftragtem und Projekt-Verantwortlichen schon während der Entwicklung aus.

¹ BVerfGE 65, 1

² <http://www.datenschutzbeauftragter-online.de/triberger-symposium-datenschutz-21-jahrhundert-realtaet-perspektive-illusion/>

über den Ablauf geplanter Projekte. Dies gilt entsprechend auch für den Kontakt zu anderen Gremien, insbesondere dem jeweiligen Personalrat, welchem im Rahmen von Mitbestimmungsverfahren eine Schlüsselposition zur Schaffung und Durchsetzung wirkungsvoller datenschutzrechtlicher Vereinbarungen und Abläufe zukommt.

Inhalte einer Datenschutzprüfung

Grundsätzlich sind bei einer datenschutzrechtlichen Prüfung sowohl rechtliche als auch technisch-organisatorische Aspekte zu berücksichtigen. Bereits durch die rechtliche Prüfung können wichtige Vorentscheidungen fallen. So nützt die wirkungsvollste Außenabschottung und das sorgfältigste Berechtigungsmanagement nichts, wenn die konkrete Verarbeitung der Daten aus rechtlichen Gründen unzulässig ist. Zunächst ist daher zu klären, ob die Daten überhaupt im gewünschten Umfang zulässigerweise erhoben, gespeichert, verändert, genutzt oder an Dritte weitergegeben werden dürfen.

Soweit die Einholung von Einwilligungen unpraktikabel ist, bedarf es einer Rechtsgrundlage.³ Fehlt eine solche, besteht im Bereich der universitären Selbstverwaltung die Möglichkeit, durch Erlass einer universitätseigenen Satzung eine geeignete Rechtsgrundlage zu schaffen. Für den Bereich der Arbeitnehmer kommt daneben der Abschluss einer Dienstvereinbarung in Betracht.⁴ Eine zunächst unzulässige Datenverarbeitung kann also durch Rechtsakte der Universität eine rechtliche Grundlage erhalten. Solche Prozesse sind jedoch aufwendig und bedürfen eines zeitlichen Vorlaufs. Zu spät bemerkt besteht die Gefahr von erheblichen Verzögerungen und Rechtsunsicherheiten. Gelingt hingegen eine frühzeitige Verständigung, inwieweit Grundlagen für die datenschutzrechtlich einwandfreie Datenverarbeitung zu schaffen sind, können die zuständigen Stellen die erforderlichen

Schritte parallel zur Entwicklung des technischen Projekts einleiten.

Bedeutsam für die rechtliche Bewertung sind im Weiteren Überlegungen zu Erforderlichkeit und Zweck der gewünschten Datenverarbeitung. Die Erforderlichkeit setzt Grenzen, indem sie die Datenverarbeitung auf das Notwendige beschränkt. Die Zweckbestimmung erlaubt die Verarbeitung personenbezogener Daten nur für die Anwendungsfälle, für welche sie auch (zulässig) erhoben worden sind.

Es liegt auf der Hand, dass beide Punkte regelmäßig erklärungsbedürftig sind. Erforderlichkeit und Zweck einer Datenverarbeitung erschließt und begrenzt sich nur zum Teil aus dem Ablauf der Datenverarbeitung selbst. Erfahrungsgemäß ergeben sich zudem im Laufe der Prozessentwicklung Änderungen. So kann die Erhebung bestimmter Daten aufgrund geänderter Prozessgestaltung oder Aufgabenzuschnitte überflüssig werden. Erforderlich wäre die Datenerhebung dann insoweit nicht mehr. Ob auf sie tatsächlich verzichtet wird, steht oft auf einem anderen Blatt.

Die rechtliche Prüfung sorgt auch für erste Weichenstellungen zum Umfang „technisch-organisatorischer Schutzmaßnahmen“. Deren Anforderungen richten sich nach der Schutzbedürftigkeit der verarbeiteten Daten. So kann sich bereits die Entscheidung, ein bestimmtes, sensibles Datum mehr oder weniger zu verarbeiten, nachhaltig auf Zulässigkeit oder zu betreibenden Aufwand auswirken.⁵

In technischer Hinsicht wichtigste Grundlage der datenschutzrechtlichen Prüfung ist das Sicherheitskonzept. Darin sind an der HU neben dem Ablauf der Datenverarbeitung die zu erwarteten Gefahren der Datenverarbeitung ebenso aufzuzählen, wie die vorgesehenen Schutzmaßnahmen. Das Sicherheitskonzept hat dabei im Wesentlichen drei Effekte:

Zunächst bildet es die Grundlage der datenschutzrechtlichen Prüfung der Datenverarbeitung. Aufgrund möglicher

Gefahren für Schutzziele, wie z. B. Vertraulichkeit oder Integrität der Daten und vorgesehener Schutzmaßnahmen, wird eine Bewertung vorgenommen, ob die mit der Datenverarbeitung einhergehenden Risiken für den Schutz personenbezogener Informationen tragbar sind oder nicht.⁶ Für die Erstellung von Sicherheitskonzepten werden interne Leitlinien entwickelt, die wiederum einem stetigen Fortschreibungsprozess unterworfen sind. Es wird so für alle Beteiligten leicht erkennbar, wo noch offene oder klärungsbedürftige Punkte gegeben sind. Allgemein ist zu sagen, dass die Prüfung umso reibungsloser vonstatten geht, je konkretere Informationen über die Einzelheiten des geplanten Verfahrens, die befürchteten Gefahren, zu den konkret verarbeiteten Daten und den vorgesehenen Schutzmaßnahmen enthalten sind. Ausführlich mit der Erstellung von Sicherheitskonzepten beschäftigt sich der Artikel von Herbst/Rauschenberg, S. 18.

Des Weiteren kann das Sicherheitskonzept auch als Instrument der Selbstüberprüfung dienen. Die bewusste Verschiebung des Fokus der Prozessbeschreibung von der Funktionalität eines IT-Verfahrens auf die Sicherheits- und Datenschutzaspekte bietet einen neuen Blickwinkel. Im Zuge der Beschreibung der Gefahren und getroffenen Sicherheitsmaßnahmen fallen so im Idealfall bereits bei Erstellung unstimme Punkte auf.

Schließlich bietet das Sicherheitskonzept eine Grundlage für die Erstellung der sogenannte Dateibeschreibung (in anderen Datenschutzgesetzen auch Verfahrensverzeichnis genannt). Diese Zusammenstellung der wichtigsten Punkte der Datenverarbeitung ist eine gesetzlich festgeschriebene Pflicht,⁷ welche die für die Datenverarbeitung verantwortliche Stelle trifft. Sie ist zudem Ausbildung des informationellen Selbstbestimmungsrechts, welches jedem Betroffenen zusteht.

3 vgl. § 6 Abs. 1 Satz BlnDSG.

4 vgl. Kommentar zum BDSG Gola/Schomerus § 4 Rn. 10.

5 vgl. hierzu z.B. die Anforderungen an die Verarbeitung „besonderer Kategorien personenbezogener Daten“ gem. § 6a BlnDSG.

6 siehe z. B. <http://www.datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet>

7 siehe § 19 BlnDSG.

Einbindung des behDSB

Bislang bedarf es – ausgehend vom Wortlaut der Datenschutzgesetze – der positiven Feststellung, dass personenbezogene Daten verarbeitet werden sollen und daher an den behDSB heranzutreten ist. Bisweilen ist es nicht eindeutig, ob Daten tatsächlich personenbezogen sind. Damit mag es als attraktive Alternative erscheinen, sich um die positive Feststellung zu drücken und die Datenverarbeitung gewissermaßen als „eigentlich nicht so richtig personenbezogen“ zu definieren. Vermeintliche Zeitfresser scheinen damit aus dem Weg geräumt. Sind die Daten gleichwohl personenbezogen, steuert man im besten Fall auf das Ausgangsszenario einer zu späten Einbeziehung des behDSB zu, im schlechtesten Falle in die Haftung aufgrund von Verstößen gegen den Datenschutz. Die Existenz eines Datenschutzverstößes beginnt nicht erst mit der Feststellung durch den behDSB. Da ein Personenbezug, wie oben beschrieben, sehr leicht gegeben ist, bleiben so erhebliche Unsicherheiten. Als Alternative bietet es sich daher an, einen fortlaufenden Austausch über Neueinführungen oder Veränderungen von IT-Prozessen zu pflegen. Die Einbindung des behDSB ergibt sich damit von selbst und kann, insbesondere wenn erkennbar keine personenbezogenen Daten verarbeitet werden, auf informellem Wege verlaufen. Zudem entsteht so frühzeitig Klarheit über die weiteren Abläufe. Dieser Ansatz wird derzeit in der Zusammenarbeit zwischen behDSB und der IT in der Verwaltung verfolgt und zeigt – für beide Seiten - sehr befriedigende Ergebnisse.

Eine in den Prozessablauf verankerte Einbindung des Datenschutzbeauftragten ist auch aus Gründen der Ressourcenplanung bedeutsam. Datenschutz funktioniert nicht von selbst. Gespräche sind vorzubereiten und erforderliche Dokumente zu erstellen. Wird der Aufwand für den notwendigen „Papierkram“ nicht von vornherein berücksichtigt, sind Projektverzögerungen strukturell bereits angelegt.

Zudem kann die Einbindung des behDSB noch unter einem weiteren Aspekt hilfreich sein, der einen Grund-

konflikt des Datenschutzes im Bereich moderner IT-Verfahren betrifft: Datenschutz baut auf Selbstbestimmung und Transparenz, während die zugrunde liegenden technischen Vorgänge immer komplexer und ineinander verwobener werden. Oder anders ausgedrückt: Im Internet zu surfen und moderne Web 2.0-Dienste zu nutzen ist mittlerweile kinderleicht. Welche personenbezogenen Daten dabei versandt, verarbeitet oder gar zweckentfremdet werden, ist auch für Experten kaum auszumachen.

Möglichkeiten zur Gewährleistung eines effektiveren Datenschutzes sind vorhanden. Jedoch sind viele der Anwendungen in ihrer Bedienbarkeit noch in einem Status, der erhebliche Kenntnisse und vor allem einen erheblichen Willen der Nutzer zum Datenschutz voraussetzt. Ziele zur Einführung neuer, datenschutzfreundlicher Anwendungen in der Universität sollten daher auch beinhalten, die Abläufe einfacher bedienbar und beherrschbar zu gestalten. Dazu gehören Schulungskonzepte ebenso wie ein Fokus auf die Berücksichtigung gleichermaßen datenschutz- wie anwenderfreundlicher Ansätze (neudeutsch Usability⁸) schon in der Konzeptionsphase. Auch hier kann der behDSB beratend zur Seite stehen.

Fazit

Der effektivste Weg, befürchteten Verzögerungen aufgrund der Einbindung des behDSB entgegenzutreten, ist – die frühzeitige Einbindung des behDSB. Auf diese Weise kann der Situation Rechnung getragen werden, dass eine Reihe notwendiger, datenschutzrechtlicher Prüfpunkte Rücksprachen und zeitlichen Vorlauf erfordern. Sonstige Befürchtungen sind häufig überzogen. Nur ein kleiner Bruchteil anfragender IT-Projekte an der HU blieb im vergangenen Jahr mit Blick auf datenschutzrechtliche Bedenken im Ergebnis unrealisiert; wenn, war dies für die Beteiligten wenig überraschend.

⁸ zum Thema Usable Security und Privacy siehe z.B.: Fischer-Hübner, Iacono, Möller, Datenschutz und Datensicherheit 2010, 773.

In der Gesamtschau fanden sich in nahezu allen Fällen Lösungen, mit denen die Projekte datenschutzkonform umgesetzt werden konnten. Teils waren keine oder nur minimale Änderungen erforderlich. Dies ist insbesondere darauf zurückzuführen, dass datenschutzrechtliche Belange und Anpassungen bereits während früher Planungsstadien Berücksichtigung fanden.