Erstellung von Verfahrensbeschreibungen

Dieses Dokument enthält Hinweise für die Erstellung einer Verfahrensbeschreibung für das Verfahrensverzeichnis und die Vorabkontrolle nach Datenschutzgesetz (DSG). Das Dokument bezieht sich dabei auf die Vorlage für Verfahrensbeschreibungen.

➔ Was sind personenbezogene Daten?

Personenbezogene Daten, sind alle Daten, die eine Person beschreiben. Damit sind auch Daten gemeint, die indirekt auf eine Person bezogen werden können. Beispielsweise kann ein Autokennzeichen als personenbezogenes Datum gesehen werden, wenn eine Person den Wagen in der Regel benutzt.

➔ Dürfen die Daten verarbeitet werden?

[Abschnitt 2 Vorlage: Zweckbestimmung und Rechtsgrundlage]

Das Datenschutzgesetz macht eine Zweckbestimmung einer Datenverarbeitung nötig:

Nach Datenschutzgesetz muss eine gesetzliche Bestimmung die Verarbeitung der personenbezogenen Daten explizit erlauben. Verordnungen genügen deshalb als Verweis nicht. Verordnungen setzen aber meist Gesetze um, auf die man sich berufen kann.

Als Ausnahme ist die schriftliche und freiwillige Einwilligungserklärung der Betroffenen vorgesehen.

➔ Wer ist betroffen?

[Abschnitt 4 Vorlage: Kreis der Betroffenen]

Für die Frage welche personenbezogenen Daten verarbeitet werden (Abschnitt 3), sollte man sich zunächst vergegenwärtigen, wessen Daten verarbeitet werden (Betroffene).

Meist ergibt sich die erste Gruppe der Betroffenen aus dem Zweck: Nutzerdaten im Bibliothekssystem → Nutzer der Bibliothek sind betroffen. Es gibt aber weitere personenbezogene Daten, die durch den Umgang mit Softwaresystemen entstehen. Hier sollte man sich Fragen, wer wird mit dem System arbeiten, ein System nutzen:

- Personal: das die Software nutzt: z.B. Anmeldedaten, Log-Dateien, Bearbeitungsstatus von Vorgängen etc.
- Zunächst unbekannte Nutzer bei Internetdiensten, die über Netzwerk-Adressen identifiziert werden können
- Administratoren: z.B. in Log-Dateien

➔ Welche Daten werden verarbeitet?
[Abschnitt 3 Vordruck: Art der gespeicherten Daten]

Wenn klar ist, wessen Daten gespeichert werden, fällt es leichter die vielfältigen Daten in einem Softwaresystem zunächst danach auszuwählen, welche personenbezogenen Daten gespeichert werden. Daten, die nicht personenbezogen sind müssen nicht aufgelistet werden.

Die personenbezogenen Daten können nach den Betroffenen gegliedert werden. Eine weitere sinnvolle Aufteilung kann nach unterschiedlichen Zwecken erfolgen („Verarbeitungen"), die sich meist auch aus den Systemkomponenten oder aus regelmäßigen Auswertungen ergeben: Ein Bibliothekssystem, besteht aus Ausleihe, Katalogisierung, Erwerbung, technische Administration, Kontenverwaltung etc.

Datenfelder in diesen Bereichen können gruppiert werden (Datenkategorien): z.B. Name und Adresse, Angaben zu Bankverbindung etc.

Bei optionalen Daten ist es sinnvoll klar zu beschreiben unter welchen Umständen die Daten verarbeitet/erfasst werden (z.B. Alternative Kontaktadresse E-Mail oder postalische Anschrift).

Für alle Daten muss sich die Notwendigkeit der Verarbeitung direkt aus dem Gesetz ablesen lassen. Man sollte sich immer die Frage stellen, ob die Verarbeitung tatsächlich notwendig ist und warum.

Folgende Arten von Daten sind besonders zu behandeln:

- **Sensible Daten (besonders geschützte Daten):** Daten über Gesinnung, politische Einstellung, Religion, Gesundheit etc.
  Sensible Daten sind explizit zu benennen und besonders zu begründen und deren Verarbeitung bedarf besonderer Sicherungsmaßnahmen.

- **Potentiell diskriminierende Daten:** Alter, Geschlecht, Herkunft etc.
  In bestimmten Bereichen, können Daten möglicherweise zu Diskriminierung führen. Auch hier ist besondere Sorgfalt notwendig.

- **Daten über Leistung oder Verhalten:** Daten, die zur Leistungs- oder Verhaltenskontrolle von Mitarbeitern geeignet sind machen auf der Basis des Personalvertretungsgesetzes eine Beteiligung der Personalvertretung notwendig.

- **Daten mit geringer Zweckbindung:** Datenfelder für unspezifische „Bemerkungen", Fotos. Offene Bemerkungsfelder dürfen personenbezogen nicht verwendet werden, da mit ihnen beliebige Daten gespeichert werden können. Falls möglich sollte auf solche Felder verzichtet werden. In Fällen, in denen die Verarbeitung notwendig ist, technische Veränderungen an Systemen aber nicht möglich sind, kann durch Verfahrensanweisungen dokumentiert werden, welche Daten in diesen Feldern gespeichert werden (dürfen). Die Mitarbeiter sind dann auf diese Verfahrensanweisung zu verpflichten.

Fotodateien sind durch die (mögliche) Verbindung zur Videoüberwachung möglichst zu vermeiden.

➔ Wer verarbeitet die Daten?
[Abschnitt 5 Vorlage: Zugriffsberechtigte Personen oder Personengruppen]

Aus der Beschreibung der Personen sollte letztlich ersichtlich sein, dass nur die Personengruppen mit den Daten umgehen können, die sich aus dem Zweck ergeben. Einzelne Personen sollten hier nicht verwendet werden sondern es sollten „Rollen" eingetragen werden. Rollen können sich aus Stellen ergeben (Administrator, Mitarbeiter Reisekostenstelle etc.). Es sollte später klar ersichtlich sein (z.B. aus der Aufgaben-/Stellenbeschreibung), wer die Daten verarbeiten darf.

➔ Welche Maßnahmen werden getroffen?
[Teil B: Sicherheitsmaßnahmen]

Für die Verarbeitung personenbezogener Daten sind Sicherungsmaßnahmen zu treffen: dazu gehören technische, wie organisatorische Maßnahmen.

Falls ein Sicherheitshandbuch existiert, das für ein Verfahren als ausreichend zu betrachten ist, kann auf dieses verwiesen werden. Speziellere Maßnahmen sind zu dokumentieren.

In Sicherheitshandbüchern sollten Maßnahmen für unterschiedliche Schutzstufen beschrieben sein. Entsprechend ist ein Verfahren in diese Schutzstufen einzuordnen. Hierbei sind die Arten der Daten zu beachten: werden sensible Daten verarbeitet, so ist eine entsprechend hohe Schutzstufe zu wählen. Zur Erstellung von Sicherheitshandbüchern sei auf das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.de) verwiesen.

Zu den Sicherheitsmaßnahmen gehören auch Verfahrensbeschreibungen, die den Mitarbeitern an die Hand gegeben werden und auf deren Einhaltung sie verpflichet werden sollten. Bei diesen Verfahren sind auch die Administratoren zu betrachten, für klar geregelt sein sollte, in welchen Fällen, sie welche Maßnahmen durchführen dürfen, wie das zu dokumentieren ist etc.

➔ Übermittlung von Daten?
[Abschnitt 6: Übermittlung bzw. Abschnitt 2: Daten und Anhang]

Als „Datenübermittlung" wird nach Gesetz der Transfer zwischen verschiedenen Stellen gesehen. Die Universität stellt als Ganzes eine solche Daten verarbeitende Stelle dar. Das bedeutet, dass die Weitergabe von Daten innerhalb der Universität nicht als Übermittlung zu sehen ist, sondern nur die Weitergabe nach außen (Strafverfolgungsbehörden, Meldeämter, andere Universitäten, Banken oder ähnliches). Eine Datenübermittlung von personenbezogenen Daten dürfte deshalb nur in den seltensten Fällen auftreten.

Die Übermittlung zwischen den Stellen innerhalb der Universität ist aber dennoch zu betrachten: Es sollte dokumentiert werden, welche Daten für weitere Zwecke und

Verfahren eingesetzt oder ausgetauscht werden. Ein solcher Datenaustausch sollte möglichst wenige Daten übermitteln und einen klaren Zweck (gesetzliche Grundlage) haben. Es sollten nur die Daten übermittelt werden die erforderlich sind. Übermittlung innerhalb der Universität sollten folgendermaßen dokumentiert werden:

- Für die Übermittlung sollte ein weiterer Abschnitt im Anhang zur Verfahrensbeschreibung eingefügt werden.
- Es sollte ein Hinweis in Abschnitt2 zur Zweckbestimmung eingefügt werden: „ Es werden für weitere Zwecke Daten an das Verfahren … übertragen."
- Bei Daten, die aus anderen Verfahren übertragen wurden, sollte im Abschnitt 3 ein entsprechender Vermerk eingetragen sein. („Aus Verfahren … übertragen.")

➔ Wie lange dürfen Daten aufbewahrt werden?
[Abschnitt 7: Fristen für Sperrung und Löschung]

Zunächst stellt sich die Frage, ob es gesetzlich vorgeschriebene Aufbewahrungsfristen für die Daten gibt. Falls nicht, so sollten die Daten gelöscht werden, sobald der Zweck der Datenverarbeitung nicht mehr besteht. Es sollte dazu dokumentiert werden, wann eine Löschung stattfindet. Die Löschfrist oder Bedingung sollte so dokumentiert sein, dass sie für den Einzelfall (Betroffene) gilt, sie sollte technisch oder organisatorisch sicherzustellen und nachprüfbar sein. (1 Monat nach Ausscheiden der Mitarbeiterin/des Mitarbeiters)

Der Datenschutzbeauftragte der Ruhr-Universität Bochum, 02/02/05