Belehrung zur Verpflichtung auf das Datengeheimnis für Mitglieder und Mitarbeiter der Piratenpartei Deutschland gem. §5 BDSG

Datenschutzverpflichtung in der Piratenpartei

Jeder, der mit persönlichen Daten der Mitglieder oder Dritter in Berührung kommt, ist vorher durch die Verantwortliche Stelle auf das Datengeheimnis zu Verpflichten. Daher ist, nach einer Belehrung / Schulung, eine sogenannte Datenschutzverpflichtung zu unterschreiben und an den Datenschutzbeauftragten des Landesverbands zu schicken.

In Bayern ist dies:
Piratenpartei Deutschland
Landesverband Bayern
Datenschutzbeauftragter
Postfach 440534
80754 München

Die Verpflichtung hat keine zeitliche Begrenzung, jedoch muss die Belehrung jährlich, durch die Verantwortliche Stelle, also in der Regel durch den DSB, erneuert werden. Wird die Belehrung nicht nachgewiesen, erlöschen alle Zugriffsrechte

Die Datenschutzverpflichtung und Belehrung innerhalb der Piratenpartei ist deutschlandweit gültig, sie wird für die Landesverbände bei den Landesdatenschutzbeauftragten verwaltet, für den Bundesverband beim Bundesdatenschutzbeauftragten, bzw. durch die Bundesgeschäftsstelle im Auftrag.

Die Datenschutzverpflichtung wirkt über das Ausscheiden hinaus.

Rechtliche Grundlagen

Hauptquellen

- Bundesdatenschutzgesetz (BDSG)
- Bayerisches Datenschutzgesetz (BayDSG)

Problematik des BDSG: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor."

Weitere Quellen

- Telemediengesetz (TMG)
- Rundfunkstaatsvertrag (RStV)
- Telekommunikationsgesetz (TKG)
- Informationsfreiheitsgesetz (IFG)
- Andere bereichsspezifische Normen
- Tarifverträge, Betriebsvereinbarungen
- …

Historie

Das erste Datenschutzgesetz in Deutschland wurde 1970 in Hessen verabschiedet.

Am 01.01.1978 trat dann das BDSG in Kraft. Es war somit eines der ersten allgemeinen Datenschutzgesetze in Europa.

1990 gab es eine Neufassung des Gesetzes, da es den verfassungsrechtlichen Anforderungen nicht genügte, was durch das Volkszählungsurteil 1983 klar wurde.

Novellierung des Gesetzes am 23.05.2001 und 03.07.2009.
Insbesondere ist die Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 erfolgt.

Ausblick

Die Europäische Union hat eine Datenschutz-Verordnung auf den Weg gebracht. Dies wird voraussichtlich das erste „Gesetz" auf europäischer Ebene sein und es ist noch ein langer Weg. Das Gesetz ist dabei nicht unumstritten.

Informationelle Selbstbestimmung

Die Basis für das Datenschutzrecht ist die informationelle Selbstbestimmung, welche im allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) definiert ist.

Das Datenschutzrecht kollidiert dabei mit anderen Grundrechten.
Recht auf integre IT; Recht am eigenen Wort; Recht am eigenen Bild; Pressefreiheit; …

Es ist daher immer eine Abwägung zwischen den kollidierenden Grundrechten.
(Siehe auch Abwägung in §28 I Nr. 2 BDSG berechtigtes Interesse gegen schutzwürdiges Interesse)

Begriffsdefinition

Personenbezogene Daten

Das BDSG definiert schutzwürdige Daten als Daten, die personenbezogen sind, oder mit Personen in Verbindung gebracht werden können.

- nicht öffentlich zugängliche Daten
- Daten für Kampagnen
- Finanzdaten
- Nutzerverhalten bei elektronischen Medien
- persönliche Vorlieben oder Abneigungen
- Zugehörigkeit zu bestimmten Gruppen

Besonders schützenswerte Daten

Dies sind nach §3 IX BDSG

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben

Verantwortliche Stelle

Eine verantwortliche Stelle (§3 VII BDSG) ist jede Person oder Stelle, die für sich selbst oder durch andere im Auftrag personenbezogene Daten verwendet.

Grundprinzipien

Prinzip der Zweckbindung

„Bei der Erhebung personenbezogener Daten sind die Zwecke, …, konkret festzulegen“ (§28 I BDSG). Der Zweck muss dokumentiert werden und ist in einer Einwilligung (§4a I BDSG) und in Auskünften an den Betroffenen anzugeben (§19 I Nr.3 BDSG). Zweckänderung ist nur in engen Grenzen möglich (§28 II BDSG)

Prinzip der Transparenz

Es muss jederzeit nachvollziehbar sein, welche Daten des Betroffenen gespeichert, verarbeitet und gelöscht werden.

Grundsatz der Direkterhebung (§4 II BDSG): Die Erhebung von personenbezogenen Daten soll direkt beim Betroffenen erfolgen.

Indirekter Anspruch des Betroffenen auf richtige Daten dadurch Recht auf Berichtigung, Löschung und Sperrung.

Prinzip der Datenvermeidung und Datensparsamkeit

Es gilt das Verhältnismäßigkeitsprinzip: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur dann erfolgen, wenn dies zur Aufgabenerledigung erforderlich ist.

Es sollten möglichst wenig personenbezogene Daten erhoben und verwendet werden. Wenn möglich, sollen Daten anonymisiert oder pseudonymisiert werden (§3a BDSG)

Prinzip der Vorabkontrolle

Bevor besonders schützenswerte Daten erhoben werden dürfen, ist eine Vorabkontrolle durch den Datenschutzbeauftragen durchzuführen. Ist kein Datenschutzbeauftragter bestellt, ist die Vorabkontrolle bei der Aufsichtsbehörde durchzuführen.

Klärende Fragen bevor Daten erhoben werden

Vor der Erhebung schutzwürdiger Daten müssen folgende Fragen im Vorfeld gestellt werden.

- Welche Daten sollen erhoben werden?
- Welche Daten sind wie zu schützen?
- Ist eine Vorabkontrolle notwendig?
- Wer arbeitet mit diesen Daten oder hat Zugriff darauf?
- Wer entscheidet über die Daten?
- Wofür werden die Daten verwendet?

Datensicherheit und IT

Was ist Datenschutz und Datensicherheit?

Als Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch. Zweck und Ziel des Datenschutzes ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jeder soll selbst bestimmen können, wem er wann welche seiner Daten und zu welchem Zweck zugänglich macht.

Datensicherheit dreht sich um die Sicherheit von legitim erhobenen Daten. Es geht darum einem Verlust oder Diebstahl der Daten entgegenzuwirken.

Gefahren in der heutigen IT

- Bußgelder, Strafverfolgung und Ersatzansprüche
- Imageverlust
- Klagen von Aufsichtsbehörden

IT-Sicherheit ist erforderlich, um Datensicherheit technisch und organisatorisch zu gewährleisten.

Gefahr des Zugriffs auf Daten

- Verlust / Diebstahl
    - Am Frankfurter Flughafen wurden allein 2008 rund 1.500 Laptops von den Reisenden einfach vergessen.
    - Nach Auskunft der Deutschen Bahn wurden allein 2007 669 tragbare Computer bei den DB-Fundbüros abgegeben.
- Viren, Phishing
- Zugriff über das Netzwerk
- Temporärer direkter Zugriff

Gegenmaßnahmen:

- Verschlüsselung
- Updates
- Firewall
- Virenscanner
- Netzwerkverschlüsselung: HTTPS, VPN
- Rechner sperren

Interne Gefahren

Gegen interne Gefahren wie Spionage, Sabotage oder Fehlbedienung sind Berechtigungs-, Zutrittssysteme, Schulungen und Backups implementiert.

Sicherheit der Daten

Das BDSG erwähnt Maßnahmen der IT-Sicherheit noch an einer anderen Stelle in §31.
Dort heißt es: „Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden."

Maßnahmen zur personellen Sicherheit

Vor der Beauftragung / Anstellung

Bevor eine Beauftragung, bzw. Anstellung stattfindet, sollen die Verantwortlichkeiten durch die Verantwortliche Stelle klar definiert sein. Diese sind in einem Protokoll oder Beschlussbuch zu dokumentieren. Außerdem muss sichergestellt sein, dass der Beauftragte, bzw. Angestellte, für die Aufgaben geeignet ist.

Während der Beauftragung / Anstellung

Es ist zu kontrollieren, dass der Beauftragte, bzw. der Angestellte, seine Verantwortlichkeiten erfüllt und die ihm zur Verfügung gestellten Daten nicht für andere Zwecke verwendet.

Dies kann durch Überprüfungen und Schulungen sichergestellt werden. Sollten sich hier Probleme aufzeigen, kann, in schwerwiegenden Fällen, ein Disziplinarverfahren eingeleitet werden.

Beendigung oder Änderung der Beauftragung /Anstellung

Nach Beendigung der Beauftragung, bzw. Anstellung, ist sicherzustellen, dass der Beauftragte, bzw. Angestellte, die erhaltenen Daten löscht oder zurückgibt. Außerdem ist sicherzustellen, dass die Accounts inaktiv geschaltet oder gelöscht werden. Laut dem bayrischen IT Admin geschieht dies leider in den wenigsten Fällen.

Datenverarbeitung im Auftrag

Werden Daten an Firmen oder andere Gliederungen der Piratenpartei weitergegeben, muss eine vertragliche Vereinbarung, welche auch die datenschutzrechlichen Bereiche abdeckt, über die Datenverarbeitung bestehen.

Dies gilt auch für alle Dienste die in Anspruch genommen werden und denen persönliche Daten übermittelt werden.

Der Datenschutzbeauftragte

Wann wird ein Datenschutzbeauftragter benötigt?

Ein DSB wird laut §4f benötigt wenn mindestens eine der folgenden Bedingungen gegeben ist.
Wenn

- sich mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
- personenbezogene Daten auf andere Weise als im obigen Punkt erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind.
- die verantwortliche Stelle eine automatisierte Verarbeitungen vornimmt,
    - die einer Vorabkontrolle unterliegt, oder
    - zum Zweck der Übermittlung, oder anonymisierten Übermittlung, oder
    - für Zwecke der Markt- oder Meinungsforschung

Ansprüche des Datenschutzbeauftragten

- Der DSB ist einem vertretungsberechtigtem Vorstandsmitglied direkt zu unterstellen (§4f III BDSG)
- Innerhalb der Fachkunde weisungsfrei (aber keine Weisungsbefugnis nach Gesetz)
- Beratung durch Aufsichtsbehörde (§38I)
- Bekommt Verfahrensverzeichnis und Berechtigungskonzept (§4gII)
- Zur Erhaltung der Fachkunde die Teilnahme an Fort- und Weiterbildungsveranstaltungen ermöglichen (Fachkunde muss vor der Bestellung erreicht worden sein)
- Unterstützung insbesondere erforderliches Hilfspersonal, Räume, Einrichtungen, Geräte und Mittel, insbesondere auch Kommunikationsmittel, die nicht der Kontrolle der verantwortlichen Stelle unterliegen (§4fIV Verschwiegenheitspflicht des DSB)

Aufgaben des Datenschutzbeauftragten (§4g BDSG)

Auf die Einhaltung des Datenschutzrechts hinwirken, insbesondere

- ordnungsgemäße Anwendung der IT prüfen
- Vorabkontrolle durchführen
- Mitarbeiter schulen
- Öffentliches Verfahrensverzeichnis für jedermann „verfügbar“ machen
- Kommunikation mit Betroffenen und Aufsichtsbehörden
- Erarbeitung von Arbeitsanweisungen, Richtlinien und Beratung
- Beratung und Fortführung des Verfahrensverzeichnis
- Erstellung und Optimierung des Datenschutz-Konzepts

Kontakt

Andreas Stürzl
http://wiki.piratenpartei.de/BY:Datenschutzbeauftragter

Bei Fragen oder Anregungen bin ich zu erreichen unter:

dsb@piratenpartei-bayern.de

dsb.piraten@datenschutz-rosenheim.de

Andreas Stürzl
Haidenholzstr. 33
83071 Stephanskirchen

Tel: +49 8036 90 80 520
Fax: +49 8036 90 80 521
Mobil +49 171 46 55 239