Datenschutzschulung für Mitglieder und Mitarbeiter

der Piratenpartei Deutschland

Formal-Foo

Datenschutzverpflichtung und Belehrung in der Piratenpartei

Jeder Pirat, der Zugriff auf persönliche Daten der Mitglieder oder Dritter erhalten soll, ist vorher:

- **zu belehren (§4g (1) 2. BDSG) und**
- **auf das auf das Datengeheimnis zu verpflichten (§5 BDSG).**

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz ... hat insbesondere

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

§ 5 BDSG Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Daher ist, nach einer Belehrung / Schulung, eine sogenannte Datenschutzverpflichtung zu unterschreiben

Link: http://wiki.piratenpartei.de/wiki/images/7/77/Datenschutzverpflichtung.pdf

und an den jeweiligen Landesverband zu senden. In NRW ist das:

Piratenpartei Deutschland
Landesverband NRW
Postfach 10 30 41, 44030 Dortmund

Die Datenschutzverpflichtung hat keine zeitliche Begrenzung.

In NRW erhalten die PIRATEN nach einer Erstbelehrung in unregelmäßigen Abständen einen Datenschutznewsletter. Eine jährliche Auffrischung im Mumble erfolgt nicht.

Teilnehmer senden mir bitte WÄHREND DER SCHULUNG eine Email

- **an markusvonkrella@piratenpartei-nrw.de**
- **gerne verschlüsselt, Open-PGP-Key 0x34082DA3**
- **mit dem Betreff: Datenschutzbelehrung**
- **mit folgenden Angaben: Bürgerlicher Vorname und Nachname, Wiki-Nick, Angabe ob Pirat ja/nein, Wohnort, Landesverband , Mailadresse**

Die Teilnehmer erhalten anschließend von mir eine formlose Teilnahmebestätigung.

Eine Liste der Teilnehmer geht von mir verschlüsselt an den Bundes-DSB der Piraten. .

Die Datenschutzverpflichtung und Belehrung innerhalb der Piratenpartei ist deutschlandweit gültig,

Die Datenschutzverpflichtung wirkt über das Ausscheiden hinaus. Unmittelbar nach Parteiaustritt sind alle Zugriffe auf personenbezogene Daten zu löschen.

Warum das alles?

Das Erheben, Nutzen und Speichern von personenbezogenen Daten ist Bestandteil aller Lebensbereiche.

Sowohl staatliches als auch wirtschaftliches Handeln hat sich durch die erweiterten technischen Möglichkeiten zur massenhaften Verarbeitung von personenbezogenen Daten verändert.

Konkret: wir haben alle genug zu verbergen (Name, Geburtsdatum, sexuelle Vorlieben, private Fotos, Bankverbindungen, Telekommunkationsdaten, politsche Meinung, religiöse Ansichten, kritische Anmerkungen über unseren Arbeitgeber u.s.w.u.s.f.) um unsere Privatspähre und unsere freie Persönlichkeitsentfaltung zu schützen.

Damit das Grundrecht auf informationelle Selbstbestimmung auch in der Informationsgesellschaft als Freiheitsrecht der Bürgerinnen und Bürger gewahrt wird, begrenzen Datenschutzgesetze sowie technische und organisatorische Maßnahmen die Verarbeitung personenbezogener Daten durch rechtliche Regelungen.

Informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Basis für das Datenschutzrecht ist die informationelle Selbstbestimmung, welche aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) abgeleitet wird:

Art 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Art 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Die informationelle Selbstbestimmung ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Es handelt sich dabei nach der Rechtsprechung des Bundesverfassungsgerichts um ein Datenschutz-Grundrecht, das im Grundgesetz nicht ausdrücklich erwähnt wird.

Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit.

Quelle: http://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung

Personenbezogene Daten sind jedoch nach Art. 8 der EU-Grundrechtecharta geschützt:

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist ein in Deutschland geltendes Grundrecht, welches vornehmlich dem Schutz von persönlichen Daten dient, die in informationstechnischen Systemen gespeichert oder verarbeitet werden und wurde durch das Bundesverfassungsgericht aus den vorgenannten Grundrechten abgeleitet.

Hauptquellen von Datenschutzgesetzen:

- Bundesdatenschutzgesetz (BDSG)
- Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)
- 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 am 03.07.2009.
Insbesondere ist die Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 erfolgt.

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

„Die Piratenpartei Deutschland kritisiert den derzeitigen Entwurf, da er die Grundrechte des Bürgers auf Datenschutz und informationelle Selbstbestimmung im Vergleich zu privatwirtschaftlichen Interessen nur unzureichend berücksichtigt“

Unter anderem hat die Bundesregierung die Verabschiedung der Verordnung noch vor der Europawahl 2014 blockiert.

Die schwarz-gelbe Koalition hat darüber hinaus vor der Bundestagswahl 2013 einen Gesetzentwurf zum Beschäftigtendatenschutz (eigentlich Beschäftigtenüberwachungsgesetz) eingebracht, welcher aber mehrfach aufgrund von öffentlicher Kritik wieder von der Tagesordnung genommen wurde.

Der beabsichtigte Arbeitnehmerdatenschutz wäre nämlich mittels dieses Entwurfes zu einem Beschäftigtenüberwachungsgesetz mutiert.

Bei Interesse:

https://ag-datenschutz.piratenpad.de/EUDatenschutzGrundverordnung

https://ag-datenschutz.piratenpad.de/GesetzesentwurfBeschaeftigtendatenschutz

Wichtige Begriffsbestimmungen

Erlaubnisvorbehalt

Das Datenschutzrecht soll den Einzelnen davor schützen, dass sein Persönlichkeitsrecht durch den Umgang mit seinen Daten beeinträchtigt wird. Deshalb enthalten die verschiedenen Datenschutzgesetze ein so genanntes Datenverarbeitungsverbot mit Erlaubnisvorbehalt, z.B. § 4 BDSG. Nach diesem datenschutzrechtlichen Grundprinzip ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Kollisionen des Datenschutzrechtes mit anderen Gesetzen

Problematik des BDSG:

Nachrangigkeit gegenüber anderen Rechtsvorschriften des Bundes:

§ 1 Zweck und Anwendungsbereich des Gesetzes

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

Das Datenschutzrecht kollidiert häufig mit anderen Grundrechten (z. B. Pressefreiheit) und anderen Gesetzen (z.B. dem Gesetz zur Kontrolle und Transparenz (KontrAG).

Beispiel:

§ 91 Abs. 2 AktG

Hier werden die Unternehmen verpflichtet, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Bei der Bewertung von Einzelfällen ist daher immer eine Abwägung zwischen den kollidierenden Grundrechten und sonstigen Gesetzen vorzunehmen.

(Siehe auch Abwägung in §28 I Nr. 2 BDSG berechtigtes Interesse gegen schutzwürdiges Interesse)

Personenbezogene, schutzwürdige und besonders schützenswerte Daten

§ (1) BDSG:

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder **bestimmbaren** natürlichen Person (Betroffener), z. B.: Name, Anschrift, Geburtsdatum).

Schutzwürdige 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

Nicht-Öffentliche Stelle:

Die Partei ist eine nicht-Öffentliche Stelle.

Die Zulässigkeit der Verarbeitung personenbezogener Daten durch Parteien wird im BDSG im dritten Abschnitt „Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen“ geregelt.

Verantwortliche Stelle:

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Also z. B.: Der Landesvorstand, der Kreisvorstand, Verwaltungs- und Finanzpiraten

Prinzip der Zweckbindung

„Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, 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).

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über... 3. den Zweck der Speicherung.

Weitere Verwendungszwecke sind unter folgenden Voraussetzungen möglich:

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist,

a) zur Wahrung berechtigter Interessen eines Dritten oder

b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und **kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat…**

§ 28 (3) erlaubt die Datenverarbeitung zu Zwecken der Werbung und des Adresshandels, wenn der Betroffene dazu eingewilligt hat.

Weitere Nutzungszwecke werden in den folgenden Paragraphen aufgeführt.

Prinzip der Transparenz

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

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher

Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

7. die Daten für eigene Zwecke gespeichert sind und a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über 1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig

gespeicherten Wahrscheinlichkeitswerte,

2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder

2. einen Bestandteil des Wahrscheinlichkeitswerts berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Fall des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,

2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,

2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,

3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist. (7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. Er ist hierauf hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden.

Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der

verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der

Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

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.

Datenverarbeitungssysteme sind bereits bei der Auswahl und Gestaltung an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erhaben, zu verarbeiten oder zu nutzen (§3a BDSG).

§ 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Prinzip der Vorabkontrolle

Bevor besonders schützenswerte Daten erhoben werden dürfen, ist eine Vorabkontrolle durch den Datenschutzbeauftragen durchzuführen.

§ 4d Meldepflicht

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für

die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

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 Verarbeitung der Daten?
- Wofür werden die Daten verwendet?

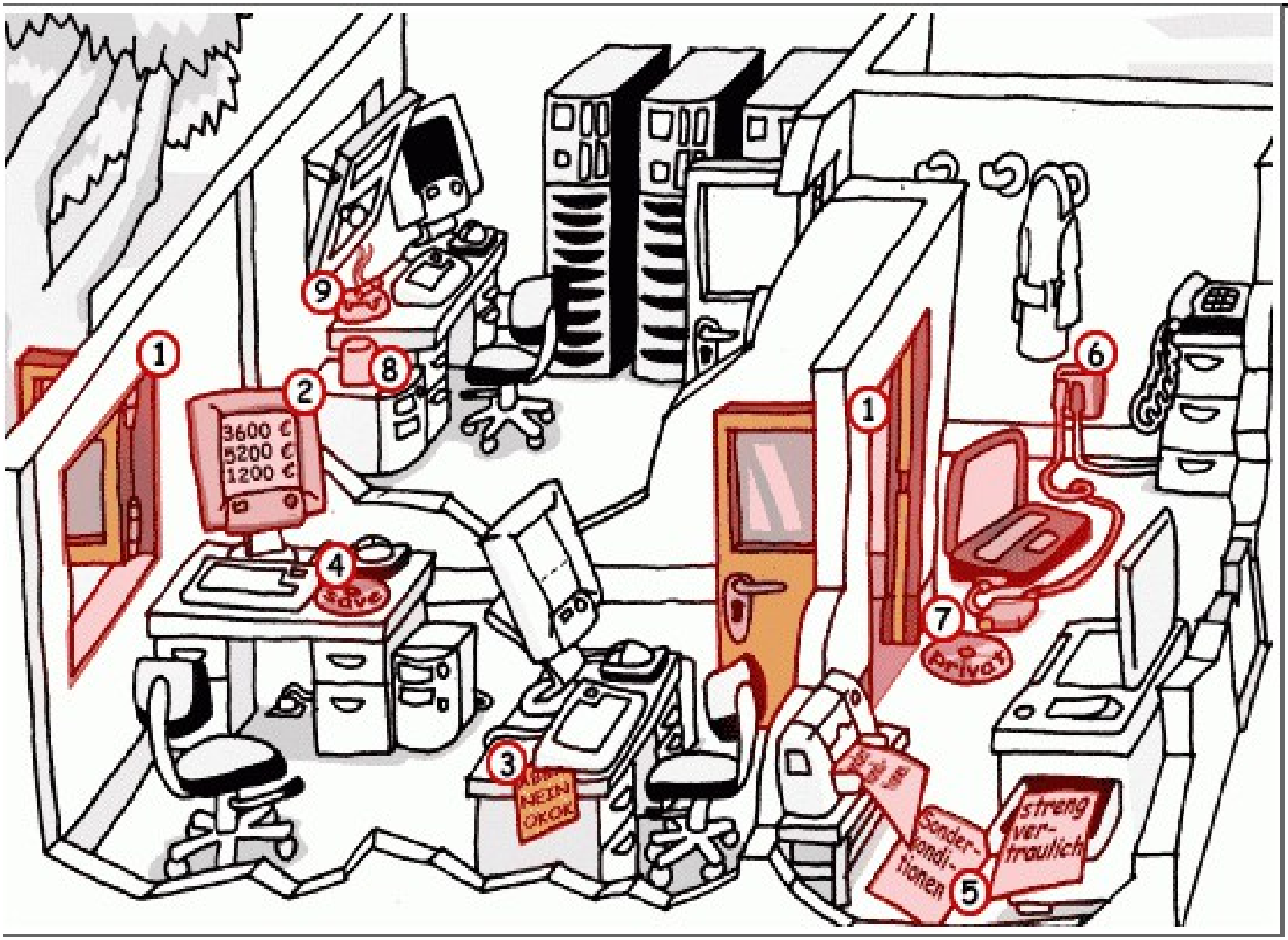
Klärende Fragen bevor Mitglieder Zugriff auf Mitgliederdaten erhalten

- Legitimation der Gliederung liegt vor?
- Bestätigung des Landesverbandes liegt vor?
- Datenschutzbelehrung gemacht?
- Datenschutzverpflichtung unterschrieben, eingesandt?
- Datenschutzverpflichtung im Verwaltungsportal eingetragen?

Datensicherheit und Informationssicherheit

Warum überhaupt Informationssicherheit

Darum:


1
2
3600 €
5200 €
1200 €
3
NEIN
OKOK
4
save
1
6
7
privat
8
9
Sonder-
kondi-
tionen
5
streng
ver-
traulich

Zahlen Daten Fakten (2010)

- 100 Milliarden Spams werden täglich weltweit zugestellt
- Über 6,5 Millionen PCs in Deutschland infiziert
- Davon 25 % Firmen-PCs
- über 4 Millionen Deutsche wurden bereits durch IT-Angriffe finanziell geschädigt
- 280 Millionen Betroffene von 2006 – 2008
- 46 % der verlorenen Daten ungeschützt
- 100 Millionen kompromitierte PCs weltweit
- davon 23 Millionen PCs aktiv in Botnetzen
- alle 2 Sekunden wird eine Schadsoftware veröffentlicht
- 12000 Notebooks gehen wöchentlich auf US-Flughäfen verloren
- 3300 Notebook gehen wöchentlich auf europäischen Flughäfen verloren
- 5000 Notebooks wurden im 1. Halbjahr 2009 in Londoner Taxen vergessen
- zwischen 40 und 80 % der Sicherheitsvorfälle werden durch interne Mitarbeiter verursacht
- immer mehr gesetzliche Verpflichtungen
- 54,9 % der Sicherheitslücken in Webanwendungen
- 74 % der Sicherheitslücken nicht gepatcht
- jeden Tag wird über Sicherheitsvorfälle in der Presse berichtet
- Der weltweite Umsatz von Internetkriminalität übersteigt mittlerweile den Umsatz durch Drogenhandel und Prostitution
- Internetkriminelle werden immer professioneller und sind mittlerweile in „Unternehmen“ organisiert
- insgesamt potenziert sich die Zahl der Schadensfälle
- die Auswirkungen der Schäden steigen
- Gefahr durch soziale Netzwerke (Facebook, YouTube etc). Enorm: 34 % der Nutzer haben bereits schlechte Erfahrungen gemacht

Was ist Informationssicherheit und wird wird das umgesetzt?

Inoformationssicherheit soll die Verfügbarkeit, Vertraulichkeit und Integrität der Daten (digital, Papier, Kopf) sicherstellen und Risiken für Schäden vermeiden.

- **Verfügbarkeit** – Informationen stehen zur Verfügung, wenn sie benötigt werden (IT-Systeme, Anwendungen, Daten)
- **Vertraulichkeit** – Informationen werden nur durch berechtigte Personen eingesehen (Geschäftsgeheimnisse, Sensible Daten, Personenbezogene Daten)
- **Integrität**: die Korrektheit und Unversehrtheit von Informationen wird sichergestellt

Näheres wird in § 9 BDSG und in der Anlage zu §9 (1) BDSG geregelt:

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. **Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.**

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder enutzt werden, zu verwehren (**Zutrittskontrolle**),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (**Trennungsgebot**).

Siehe hierzu auch die Website des BSI:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html;jsessionid=173AE650BEE5D261E2F39E844E1F83AC.2_cid294

Mögliche Schäden durch Datenverluste

- Finanzielle Verluste durch:
  - Bußgelder bis 300.000 € (eine Überschreitung des Rahmens ist im Einzelfall möglich)

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen §34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht

vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, 5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

- Ersatzansprüche, Gerichtskosten
- Wiederherstellung von Daten & Forensische Maßnahmen
- Imageverlust
- Strafverfolgung

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen

anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder

mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche

Gefahren für Datenverluste (Beispiele)

- Spionage & Datenklau
- organisatorische Mängel
- technisches Versagen
- menschliche Fehlhandlungen
- vorsätzliche Handlungen
- Viren & Würmer
- Trojanische Pferde & Spyware
- Phishing-Techniken und Botnets
- Hoaxes, Dialer, Spam, Hacks etc.
- höhere Gewalt
- etc.

Anteil	Gefahrenpotenziale	Beispiele
31%	vorsätzliche Handlungen	Manipulation, Diebstahl, Vandalismus, Missbrauch, Trojanische Pferde
30%	organisatorische Mängel	fehlende Regelungen, keine Kontrolle, unbefugter Zutritt
20%	menschliches Fehlverhalten	Fehlerbedienung, fehlerhafte Administration, Übertragen falscher Datensätze
15%	technisches Versagen	Ausfall Stromversorgung, Netzkomponenten, Datenverlust
3%	höhere Gewalt	Ausfall, Blitz, Feuer, Wasser,

Datenskandale

Http://www.projekt-datenschutz.de

Schutzmaßnahmen

Anteil	Schutzmaßnahmen
37%	Organisation
28%	Hard- und Software
13%	Kommunikation
9%	Notfallvorsorge
6%	Infrastruktur
6%	Personal

Nur 28% der Schutzmaßnahme betreffen technische Maßnahmen (IT-Systeme und Anwendungen)!

Technische Gegenmaßnahmen (Beispiele):

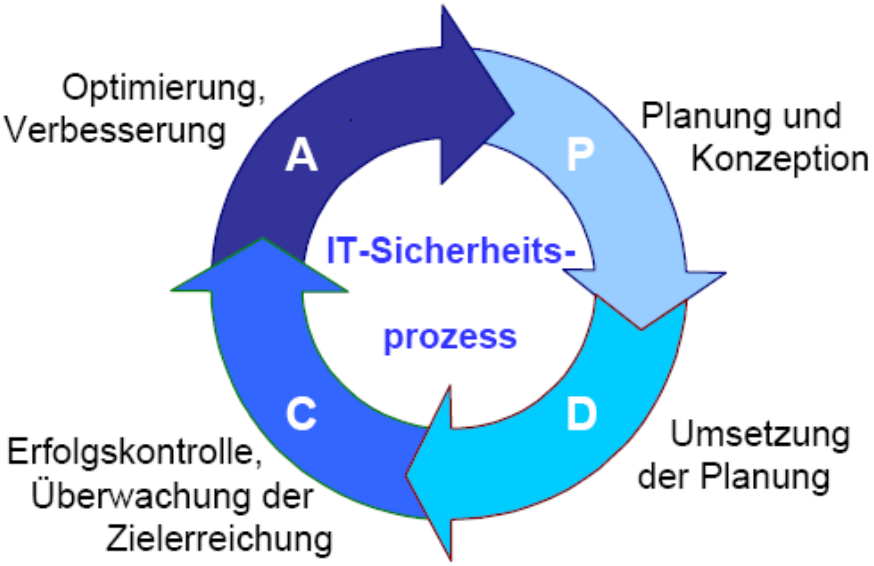
- Verschlüsselung
- Updates
- Firewall
- Virenscanner
- Netzwerkverschlüsselung: HTTPS, VPN
- Rechner sperren
- Zutrittskontrollsysteme
- Backups
- Intrusion Detection
- Data Leak Prevention

Organisatorische Maßnahmen (Beispiele)

- Sicherheitsorganisation etablieren
- Erstellung von Sicherheitsrichtlinien, Datenschutzkonzepten
- Schulungen
- Berechtigungskonzepte
- Vorabkontrolle

Fazit und Begründung, warum technische Maßnahmen allein nicht ausreichen:

Insgesamt ist Datenschutz und Informationssicherheit ein Prozess:



Datenverarbeitung im Auftrag

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

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

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 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

Markus Wetzler aka markusvonkrella
Piratenpartei Kaarst, Landesverband NRW
Landesbeauftragter für den Datenschutz der Piraten NRW
Request-Tracker: datenschutz@piratenpartei-nrw.de
Mail: markusvonkrella@piratenpartei-nrw.de
Telefon 02131/1513366
Mobil 01578/6805685
OpenPGP-Key: 0x34082DA3

http://wiki.piratenpartei.de/NRW:Datenschutzbeauftragter
http://wiki.piratenpartei.de/Benutzer:Markus_von_Krella
https://www.twitter.com/markusvonkrella
http://www.facebook.com/karlesforst
http://www.facebook.com/Piratenpartei.Kaarst
https://www.twitter.com/Piraten_Kaarst
http://www.piratenpartei-kaarst.de