



Der Bundesbeauftragte für
den Datenschutz

Belehrung zur Verpflichtung auf das Datengeheimnis für Mitglieder und Mitarbeiter der Piratenpartei Deutschland gem. §5 iVm. §4g Abs. 1 Zif. 2 BDSG

Der Bundesbeauftragte für den Datenschutz
der Piratenpartei Deutschland
Sebastian Krone aka „Bastian“
Am Bürohochhaus 2-4 - D-14478 Potsdam
Tel. 0331-281 298 200 - Fax. 0331-281 298 202
E-Mail: bundesbeauftragter@piraten-dsb.de
Twitter: BDSBPiraten
PGP-Key: 0x75F6AB8A

Was ist Datenschutz und Datensicherheit?

- „Vertrauen ist der Anfang von Allem“
(Werbесlogan der Deutschen Bank)
- „Vertrauen ist gut, Kontrolle ist besser“
(Wladimir Iljitsch Uljanow – Lenin)



Der Bundesbeauftragte für
den Datenschutz

Was ist Datenschutz und Datensicherheit?

- Datenschutz und Datensicherheit macht Sinn und Spaß!
- Datenschutz und Datensicherheit sorgen für ruhigen Schlaf in der Nacht!

Datenschutz – Rechtliche Grundlagen



Der Bundesbeauftragte für
den Datenschutz

- Archivgesetze des Bundes und der Länder
- Bundesdatenschutzgesetz (BDSG)
- DNA-Identitätsfeststellungsgesetz (ÄndGzur StPO)
- Gendiagnostikgesetz
- Gesetz zur Förderung der Steuerehrlichkeit (ÄndGzur AO)
- Informationsfreiheitsgesetz (IFG)

Datenschutz – Rechtliche Grundlagen



Der Bundesbeauftragte für
den Datenschutz

- Informationsfreiheitsgesetze der Länder (BB, BER, HB, HAM, MV, NRW, SH, SL)
- Landesdatenschutzgesetze
- Sozialgesetzbuch X
- Staatsvertrag über Mediendienste (MDStV)
- Stasi-Unterlagen-Gesetz (StUG)

Datenschutz – Rechtliche Grundlagen



Der Bundesbeauftragte für
den Datenschutz

- Teledienstedatenschutzgesetz (TDDSG)
- Teledienstegesetz (TDG)
- Telekommunikationsgesetz (TKG)
- Telekommunikations-Überwachungsverordnung (TKÜV)
- Telemediengesetz (TMG)

Datenschutz – Rechtliche Grundlagen



Der Bundesbeauftragte für
den Datenschutz

- Umweltinformationsgesetz (UIG)
- Verbraucherinformationsgesetz (VIG)
- Volkszählungsurteil

Schutz des Persönlichkeitsrechts

Das BDSG definiert schutzwürdige Daten als Daten, die personenbezogen sind oder mit Personen in Verbindung gebracht werden können. Dazu zählen z.B. auch Daten wie

- Nutzerverhalten bei elektronischen Medien
- persönliche Vorlieben oder Abneigungen
- Zugehörigkeit zu bestimmten Gruppen
- Daten um Mitarbeiter zu bewerten

Definition schutzwürdiger Daten



Der Bundesbeauftragte für
den Datenschutz

- Zusätzlich sollten in der Datensicherheit aber natürlich auch weitere Datengruppen geschützt werden. Dazu gehören z.B.
- nicht öffentlich zugängliche Daten
- Daten für Kampagnen
- Finanzdaten

Definition schutzwürdiger Daten



Der Bundesbeauftragte für
den Datenschutz

Bei der Definition schutzwürdiger Daten entstehen einige Fragen, die im Vorfeld geklärt werden müssen.

- Welche Daten sind vorhanden?
- Welche Daten sind zu schützen?
- Wer arbeitet mit diesen Daten oder hat Zugriff darauf?
- Was wird mit den Daten gemacht?
- Wer entscheidet über die Daten?

Definition schutzwürdiger Daten



Der Bundesbeauftragte für
den Datenschutz

Bei der Durchsicht ist auf Daten mit Verarbeitungsbeschränkungen nach §3 Abs. 9 BDSG zu achten („Giftschrankdaten“):

- Angaben über ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Parteizugehörigkeit
- Gesundheit
- Sexualleben

Gefahren in der heutigen IT (1/3)

Ein effektiver Datenschutz reduziert nicht nur gewisse Risiken, sondern kann auch eine positive Außenwirkung haben. Große Unternehmen nutzen ihre Anstrengungen im Bereich des Datenschutzes auch vertrieblich. Die Risikovermeidung beschränkt sich dabei meist auf die folgenden Bereiche:

Gefahren in der heutigen IT (2/3)

- Bußgelder, Strafverfolgung und Ersatzansprüche
- Imageverlust
- Verlorene oder doppelte Investitionen wegen Nichtbeachtung von Datenschutzvorschriften
- Einstellung von Prozessen (z. B. Abschaltung von Servern) durch Aufsichtsbehörden

Gefahren in der heutigen IT (3/3)

- IT-Sicherheit ist erforderlich, um Datenschutz technisch und organisatorisch zu gewährleisten. 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.“
Das BDSG erlaubt daher die Speicherung aus Gründen der IT-Sicherheit (z.B. Logs)

Datensicherheit & IT



Der Bundesbeauftragte für
den Datenschutz

Gefahrenbereich	Gefahr	Lösungsansatz
Notebooks	Diebstahl	Verschlüsselung
Externe Speichermedien	Diebstahl, Kopie, Viren	Verschlüsselung
Netzwerk	Zugriff von außen	Firewall
W-LAN	Zugriff von außen	z.B. Verschlüsselung
Tagungsräume	Zugriff aufs Netzwerk	z.B. Absicherung der Anschlüsse
E-Mail	Viren, Phishing	Virenschanner, Signatur

Gefahrenstatistik zu Notebooks, PDAs, mobilen Endgeräten:

- Laut einer Analyse von Gartner sind 57 % aller erfolgreichen Netzwerkangriffe auf einen Notebook-Diebstahl zurückzuführen.
- 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.
- Notebook-Diebstahl ist das zweithäufigste Computerverbrechen.

Physische Absicherung:

- Wichtige Komponenten, Systeme und Bereiche in einer Organisation sollten immer gegen unbefugten Zugang gesichert sein. Dies gilt z.B. für
- Serverschränke, Netzwerkdosen
- Mobile Geräte wie Notebooks, Handys, PDAs Smartphones, usw.
- Netzwerkkomponenten wie Switches, Router, Firewalls usw.
- Fax und Kopierer (mit Speicher), Hauspost, Mülleimer

Backup: (1/2)

- Backupsysteme schützen vor Datenverlust und sichern eine schnelle Verfügbarkeit im Falle eines Defekts. Ein gutes Backupsystem sollte folgende Punkte beachten:
- Es sollte auf verschiedenen Medien gesichert werden.
- Die Daten sollten verifiziert werden.
- Die Medien sollten an verschiedenen Orten gelagert werden (nicht im Serverschrank, nicht im Schreibtisch, eher zuhause - wenn im Safe).

Backup: (2/2)

- Die Daten sollten schnell und sicher wieder herstellbar sein.
- Regelmäßige Prüfung auf Wiederherstellbarkeit der Backups.

Redundanz:

- Erstellung einer Kosten/Nutzen Rechnung.
- Welcher Schaden kann bei Ausfall einer Komponente entstehen? Dies kann man dann einfach in Relation zu den Kosten stellen.
- Wie können Gliederungen hier zusammenarbeiten?

Die Sicherheit ist durch klare Richtlinien definiert:

- Nutzung von Notebooks / PDAs / Handys / Smartphones
- Nutzung WLAN, VPN oder externen Verbindungen
- Umgang mit Passwörtern
- Surfen im Internet / Nutzung von E-Mail
- Umgang im Schadensfall

- Arbeiten am PC
 - Zugang zum PC
 - Abwehr von Malware (z.B. Computerviren)
 - Verschlüsselung von Daten
 - Passwortsicherheit
- Sicheres Löschen von Daten
- Umgang mit Wechseldatenträgern

Datenschutzverpflichtung

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 eine sogenannte **Datenschutzverpflichtung nach erfolgter Belehrung** zu unterschreiben.

Für die Belehrungen sind die Datenschutzbeauftragten zuständig (§ 4g Abs 1 Zif. 2 BDSG)

Datenschutzverpflichtung

- Diese Verpflichtung unterliegt einer jährlichen Belehrung durch den DSB der verantwortlichen Stelle. Wird die Belehrung nicht nachgewiesen, erlöschen alle Zugriffsrechte automatisch.
- Die Datenschutzverpflichtung **wirkt über das Ausscheiden hinaus**.

Zusammenfassung:

- Durch ein Datenschutzkonzept werden die individuellen Faktoren der IT-Sicherheit berücksichtigt (zumindest die folgenden drei Bereiche):
 - Anweisungen für den Schadensfall
 - Organisatorische Absicherung
 - Technische Absicherung

Was ist Informationssicherheit?



Der Bundesbeauftragte für
den Datenschutz

Was ist Informationssicherheit?

- Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Werten unabhängig von Ihrer Form.
- Daten sind alle schriftliche, bildliche und gesprochene Informationen.

Was ist Informationssicherheit?



Der Bundesbeauftragte für
den Datenschutz

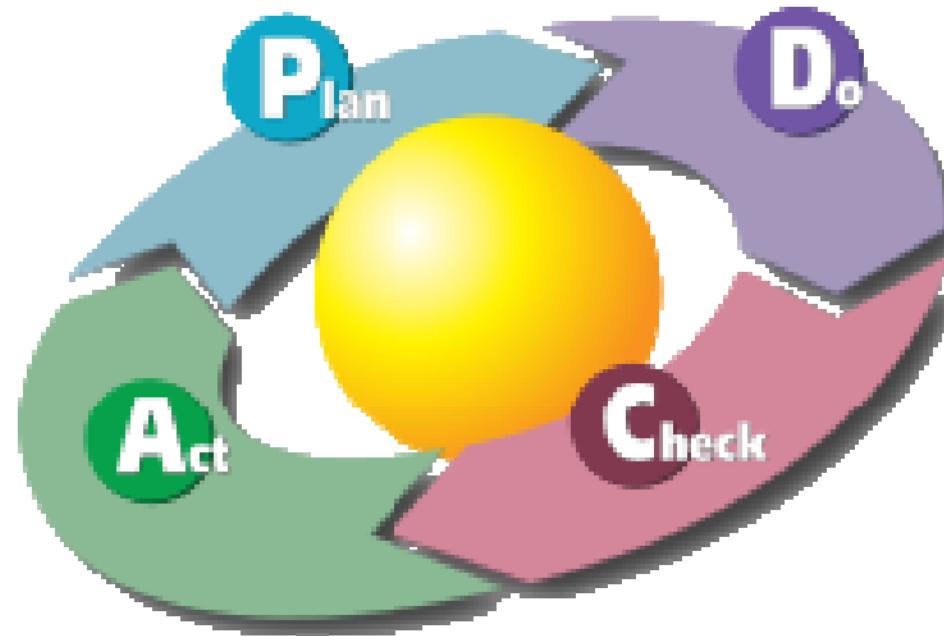
- **Vertraulichkeit:**
Unberechtigten Personen, Einheiten oder Prozessen dürfen Informationen nicht verfügbar oder zugänglich gemacht werden.
- **Integrität:**
Werte müssen richtig und vollständig sein
- **Verfügbarkeit:**
Daten einer berechtigten Einheit auf Anforderung zugänglich und nutzbar machen.

Was ist Informationssicherheit?



Der Bundesbeauftragte für
den Datenschutz

- plan- do – check - act:



Belehrung zur Verpflichtung auf das Datengeheimnis gem. §5 BDSG



Der Bundesbeauftragte für
den Datenschutz

• Kleine Pause



Maßnahmen zur personellen Sicherheit

1. Vor der Anstellung/Beauftragung

- **Ziel:** Sicherstellung, dass Angestellte, Auftragnehmer, Dritte ihre Verantwortlichkeiten verstehen und für die Aufgaben geeignet sind. Diebstahl, Betrug- und Missbrauchsrisiko verringen.
- **Umsetzung:** Überprüfung vor der Anstellung/Beauftragung im Rahmen der gesetzlichen Möglichkeiten, Vertragsklauseln und Verhaltensregeln.

Maßnahmen zur personellen Sicherheit

2. Während der Anstellung/Beauftragung

- **Ziel:** Sicherstellung, dass sich alle Ihrer Verantwortlichkeiten und der Bedrohungen bewusst sind und danach handeln.
- **Umsetzung:** Regelmäßige Überprüfung und Schulung, Disziplinarverfahren.

Maßnahmen zur personellen Sicherheit

3. Beendigung oder Änderung der Anstellung/Beauftragung

- **Ziel:** Sicherstellung, dass die Beauftragung bzw. das Mitarbeiterverhältnis ordnungsgemäß beendet bzw. die Anstellung/ Beauftragung gewechselt wird.
- **Umsetzung:** Verantwortlichkeiten für Änderungen festlegen (Zugriffsrechte / Rückgabe Computer).

Physische und umgebungsbezogene Sicherheit

1. Sicherheitsbereiche (*nur bedingt aktuell*)

- **Ziel:** Schutz vor unerlaubtem Zutritt, Beschädigung und Störung der Infrastruktur und der Informationen der Organisation.
- **Umsetzung:** Sicherheitszonen, Zutrittskontrollen, Sicherung von Büros, etc. Schutz gegen Umwelteinflüsse (Feuer, Wasser, etc)

2. Sicherheit von Betriebsmitteln

- **Ziel:** Verhinderung von Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und den zugehörigen Systemen.
- **Umsetzung:**
Schutz (unerlaubter Zugriff),
Versorgungseinrichtungen (Notstrom, USV),
Verkabelung (Anzapfen), Instandhaltung
(Verfügbarkeit auf Datenzugriff gewährleisten).
Sichere Entsorgung (z.B. Festplatte).

Betriebs- und Kommunikationsmanagement

1. Verfahren und Verantwortlichkeiten

- **Ziel:** Korrekter und sicherer Betrieb der Informationsverarbeitenden Einrichtungen.
- **Umsetzung:**
Dokumentierte Betriebsprozesse einschl.
Änderungsverwaltung, Verantwortlichkeiten
Trennung von Test- und Produktiveinrichtungen

2. Management der Dienstleistungserbringung von Dritten (1/2)

- **Ziel:** Aufrechterhaltung der Informationssicherheit bei gleichzeitiger Sicherstellung der Dienstleistungserbringung entsprechend der Liefervereinbarung.
- **Umsetzung:**
Regelmäßige Überwachung und Überprüfung der Einhaltung

Betriebs- und Kommunikationsmanagement

2. Management der Dienstleistungserbringung von Dritten (1/2)

Beispiele an der Praxis:

- Steuerberater
- Druckdienste / Copycenter (z.B. Einladungen)
- Softwarewartung

3. Systemplanung und Abnahme

- **Ziel:** Das Risiko von Systemfehlern und Systemausfällen zu minimieren.
- **Umsetzung:**
Kapazitätsplanung (Serverüberlastung)
System-Abnahme (Kriterien definieren zur Abnahme / Was muss es können?)

4. Schutz vor Schadsoftware

- **Ziel:** Schutz der Integrität von Software und Informationen.
- **Umsetzung:** Maßnahmen gegen Schadsoftware, Regelung für mobilen Programmcode (Java, JavaScript, ActiveX)

5. Backup

- Ziel: Schutz der Integrität von Software und Informationen.
- Umsetzung: Erstellung von Backup

6. Management der Netzsicherheit

- **Ziel:** Informationen in Netzen und Infrastruktur zu schützen.
- **Umsetzung:** Angemessene Verwaltung und Kontrolle von internen und externen Netzen Sicherheitseigenschaften und Admin-anforderungen für alle Netze definieren

7. Handhabung von Speicher- und Aufzeichnungsmedien

- **Ziel:** Unerlaubte Veröffentlichung, Veränderung, Zerstörung von Informationen und Systemen (Assets) sowie Störung des Partei- und Geschäftsbetriebs verhindern.
- **Umsetzung:** Verwaltung von Wechselmedien (Verfahrensanweisungen), Entsorgung von Medien, Umgang mit Informationen (Verfahren für Umgang und Speicherung von Informationen festlegen).

8. Austausch von Informationen

- **Ziel:** Sicherheit von Informationen und Software, die intern und extern ausgetauscht werden.
- **Umsetzung:** *Regeln festlegen* (z.B. was wird wie und wann verschlüsselt).
Physische Medien und elektronische Nachrichten schützen.

9. E-Commerce-Anwendungen

- **Ziel:** Sicherheit und sichere Benutzung von E-Commerce.
- **Umsetzung:** E-Commerce und Online-Transaktionen schützen.

10. Überwachung

- **Ziel:** Aufdeckung nicht genehmigter, informationsverarbeitender Aktivitäten.
- **Umsetzung:**
Protokolle (auch zur Beweissicherung)
Zeitsynchronisation (gemeinsame Referenzzeit)

Zugangskontrolle

1. Anforderungen für Zugangskontrolle

- **Ziel:** Kontrolle des Zugangs zu Informationen.
- **Umsetzung:** *Regelwerk* zur Zugangskontrolle

2. Benutzerverwaltung

- **Ziel:** Sicherstellung des Zugangs zu Informationssystemen / Verhindern von Zugang durch Unbefugte.
- **Umsetzung:**
Benutzerregistrierung
Verwaltung und Überprüfen von Rechten und Passwörtern

3. Benutzerverantwortung

- **Ziel:**
Verhinderung von unbefugtem Zugriff, Diebstahl, Kompromittierung von Informationen.
- **Umsetzung:**
Passwortverwendung (Sicherheitsregeln für Auswahl und Anwendung von Passwörtern).
Unbeaufsichtigte Technik schützen (Bildschirmsperre).
Aufgeräumter Schreibtisch (keine wichtigen Informationen offen liegen lassen, Papierkorb)
„Leerer Monitor“

4. Zugangskontrolle für Netze

- **Ziel:** Verhinderung von unbefugtem Zugang zu Netzdiensten.
- **Umsetzung:**
Regeln zur Nutzung von Netzen
Technische Möglichkeiten beachten und nutzen
(Routingkontrolle etc.), VPN (Zertifikate)

5. Zugriffskontrolle auf Betriebssysteme

- **Ziel:**
Verhinderung von unbefugtem Zugriff auf das Betriebssystem.
- **Umsetzung:**
Sichere Anmeldung, Benutzerauthentisierung, Passwortverwaltung
Dienstprogramme einschränken / kontrollieren
Session Time-out.

6. Zugangskontrolle zu Anwendungen und Information

- **Ziel:**

Verhinderung des unbefugten Zugangs zu Informationen in Anwendungssystemen.

- **Umsetzung:**

Einschränkung von Informationszugriff
(benutzerspezifische Zugangskontrolle)

Isolation sensibler Systeme

7. Mobile Computing und Telearbeit

- Ziel:
Sicherstellen der Informationssicherheit bei mobile Computing und Telearbeit (z.B. Zugriff auf die Mitgliederdatenbank).
- Umsetzung:
Regelungen, Leitlinien und Maßnahmen zur sicheren Nutzung (VPN, Zertifikate).

Umgang mit Informationssicherheitsvorfällen

1. Melden von Informationssicherheitsereignissen und Schwachstellen

- **Ziel:** Schwachstellen in Informationssystemen müssen gemeldet werden, sodass rechtzeitig reagiert werden kann.
- **Umsetzung:**
Verpflichtung zur Meldung für Schwachstellen für Alle (intern und extern).
Sicherstellung der geeigneten Kommunikationswege (Managementkanäle).

2. Umgang mit Informationssicherheitsvorfällen und Verbesserungen

- Einhaltung eines **einheitlichen und effektiven** Ansatzes zum Umgang mit Informationssicherheitsvorfällen.
- Umsetzung (1/2):
Verantwortlichkeiten für den Umgang mit Vorfällen festlegen
Das Lernen aus den Vorfällen sicherstellen
Sammeln von Beweisen

Informationssicherheitsaspekte bei der Sicherstellung des Partei- und Geschäftsbetriebes

Umsetzung (2/2):

Gelenkter Prozess zur Sicherstellung des Betriebs.

Identifizierung und Risikobetrachtung von Ereignissen die den Betrieb stören können.

Notfallpläne, Rahmenwerk für die Notfallpläne festlegen (Widersprüche vermeiden).

Regelmäßiges Testen, Überprüfen und Neubewerten der Notfallpläne.

- **Desaster Recovery Management**

Einhaltung von Vorgaben (Compliance)

1. Einhaltung gesetzlicher Vorgaben

- **Ziel:** Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen, sowie gegen Sicherheitsanforderungen.
- **Umsetzung:**
Identifikation der relevanten Gesetze.
Schutz von Rechten Dritter. Beachtung von Lizenzen bei Software.
Datenschutz und Vertraulichkeit, Verhinderung von Missbrauch.

2. Einhaltung von Sicherheitsregelungen und – standards, und technischer Vorgaben

- **Ziel:** Sicherstellung, dass Systeme die Sicherheitsregelungen und - standards einhalten.
- **Umsetzung:**
Vorstände und Beauftragte müssen in Ihrem Verantwortungsbereich die Einhaltung sicherstellen.
Regelmäßige Prüfung der Einhaltung der Vorgaben.

3. Überlegungen zu Revisionsprüfungen von Informationssystemen

- **Ziel:** Steigerung der Effektivität und Minimierung der Störungen bei Revisionsprozessen für Informationssysteme.
- **Umsetzung:**
Sorgfältige Planung von Revisionsprozessen, um Störungen der Prozesse zu vermeiden.
Missbrauch von Tools zur Untersuchung von Informationssystemen vermeiden.

Beispiele für die Notwendigkeit für eine DSV

- Admins, Moderatoren, Beauftragte mit Zugriff auf persönliche Daten, technisches Personal
- Mailinglisten-Admins und -Mods
- Forum-Admins, -Moderatoren,
- Blog (z. B. Wordpress) -Admins, -Redakteure (wenn E-Mails gespeichert werden)
- Vorstände
- Kassenprüfer
- Rechnungsprüfer (Belehrung kann entfallen)

Besonderheiten bei Mailinglisten



Der Bundesbeauftragte für
den Datenschutz

- Mitgliederliste darf nur für den Admin einsehbar sein.
([https://service.piratenpartei.de/admin/\[listenname\]/privacy](https://service.piratenpartei.de/admin/[listenname]/privacy)) „*Mitgliedschaft anzeigen*“
- Archivierung muss ausgeschaltet sein, es sei denn alle Mitglieder haben dem zugestimmt.
([https://service.piratenpartei.de/admin/\[listenname\]/archive](https://service.piratenpartei.de/admin/[listenname]/archive))
- Zugangspasswort darf nur an jemand weitergegeben werden, der eine DSV unterschrieben hat und belehrt wurde.

Verweise

- BSI: Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Home/home_node.html

BSI-Grundschutzkatalog:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html

BSI-Notfallmanagement (Desaster Recovery Management)

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01003.html

- Datenschutz-WIKI

http://www.bfdi.bund.de/bfdi_wiki/index.php/Hauptseite

- Verfahrensverzeichnisse (Informationssicherheit)

<http://www.verinice.org>



Der Bundesbeauftragte für
den Datenschutz

Vielen Dank für die Aufmerksamkeit!

Der Bundesbeauftragte für den Datenschutz
der Piratenpartei Deutschland

Sebastian Krone aka „Bastian“
Am Bürohochhaus 2-4 - D-14478 Potsdam
Tel. 033766-21363 - Fax. 033766-205877

E-Mail: bundesbeauftragter@piraten-dsb.de
<http://www.piraten-dsb.de>

oder

<https://wiki.piratenbrandenburg.de/Bundesdatenschutzbeauftragter>

Twitter: BDSBPiraten

PGP-Key: 0x75F6AB8A