

Inhaltsverzeichnis

1	Datenschutzrichtlinie	1
1.1	Zugriff	1
1.2	Speicherung	2
1.3	Übermittlung	2
1.4	Transport	3
1.5	Drucken	3
1.6	Herausgabe	3
1.7	Sprechen	4

1 Datenschutzrichtlinie

Diese Richtlinie wurde in Zusammenarbeit mit dem Vorstand der Piratenpartei Schweiz und deren Geschäftsprüfungskommission erstellt. Die Befolgung stellt sicher, dass die Mitgliederdaten den Schutz geniessen, der ihnen würdig ist. Es gilt der Grundsatz: «So wenig wie möglich und nur wenn wirklich notwendig.» Die Regeln lassen sich in verschiedene Arten des Umgangs unterteilen.

1.1 Zugriff

Wir sind gesetzlich verpflichtet, den Kreis der Zugriffsberechtigten so tief wie möglich zu halten. Deshalb gelten die folgenden einfachen und strikt zu befolgenden Regeln:



- Gewähre niemanden Zugriff auf die Mitgliederdatenbank. Der Zugriff muss von der Piratenpartei Schweiz für jede einzelne Person gewährt werden.
- Greife nicht auf die Mitgliederdatenbank zu, ausser es ist für die Erfüllung der Geschäfte notwendig.
- Frage nur die Daten (Personen und Attribute) ab, die du wirklich brauchst.

1.2 Speicherung

Für die Speicherung von Daten bestehen viele Möglichkeiten. Bei Befolgung der folgenden Regeln ist ein hoher Sicherheitsstandard gewährleistet.

- Speichere keine Personendaten ab, ausser es ist wirklich notwendig.
- Speichere nur so wenig Daten (Personen und Attribute) wie notwendig ab.
- Speichere die Daten nur so lange, wie sie benötigt werden.
- Verschlüssele die Daten mit TrueCrypt oder einem gleichwertigen Tool.
 - Wähle eine sichere Passphrase (Sonderzeichen und Zahlen sowie möglichst viele Zeichen).
 - Lass den TrueCrypt Container nur so lange offen, wie wirklich notwendig.
- Stelle sicher, dass niemand ausser du selber Zugriff auf die gespeicherten Daten erhält.
 - Sperre deinen Rechner, wenn du dich von ihm entfernst.
 - Verschlüssele die gesamte Festplatte deines Notebooks.
- Schliesse Datenträger mit Personendaten weg, trage sie auf dir, oder beaufsichtige sie.
- Vernichte oder überschreibe Datenträger, auf denen Personendaten gespeichert waren.

1.3 Übermittlung

Bei der Übermittlung von Daten müssen die folgenden Punkte berücksichtigt werden. Es reicht nicht, ein Protokoll mit Verschlüsselung (z.B. SSL) zu verwenden!



- Übermittle keine Personendaten, ausser es ist wirklich nötig.
- Übermittle nur so wenig Daten (Personen und Attribute) wie nötig.
- Übermittle nur über sichere Verbindungen (HTTPS, SCP, ...).
- Benutze Authentifizierung und Verschlüsselung mit GPG oder einem gleichwertigen System.
 - Halte deinen privaten Schlüssel geheim.
 - Wähle eine sichere Passphrase.
 - Prüfe die öffentlichen Schlüssel deines Gegenübers (Fingerprint).

1.4 Transport

- Siehe Speicherung.

1.5 Drucken

Es gibt nur wenige Situationen, in denen ein Ausdruck von Mitgliederdaten tatsächlich notwendig ist. Sollte dies der Fall sein (z.B. Akkreditierungsliste), gelten die folgenden Regeln:

- Drucke Personendaten nur aus, wenn es nötig ist.
- Drucke nur die Daten aus, die du wirklich auf Papier benötigst.
- Schliesse Ausdrücke von Personendaten weg, trage sie auf dir, oder beaufsichtige sie.
- Vernichte Ausdrücke, die du nicht mehr benötigst (Schredder).

1.6 Herausgabe

Die Mitgliedschaft in einer Partei gilt als besonders schützenswertes Datum und ist somit entsprechend vertraulich zu behandeln. Es dürfen also grundsätzlich nur mit Einwilligung der betroffenen Person Daten herausgegeben werden. Ausserdem ist folgendes zu berücksichtigen:

- Gib keine Daten ohne ausdrücklichen Auftrag heraus.



- Stelle sicher, dass die Daten nur an diejenigen (Post, Mailserver) herausgegeben werden, die sie benötigen.
- Gibt nur so wenig Daten wie nötig heraus.

1.7 Sprechen

Achtung: Im Zug, in Büros, in der Öffentlichkeit und selbst zu Hause sind oft unerwartete Beobachter bzw. Lauscher. Vergewissere dich also, dass dir niemand zuhört.

- Sprich nicht über Personendaten, ausser mit Personen, die ebenfalls Zugriff darauf haben.

