

4. Dresdner Forum für Notarrecht, 29. Juni 2012

Schutz notarieller Verschwiegenheit: Datenschutz und Datensicherheit im Notariat

Marius Klingler
Notarassessor

Inhalt

01

Einführung

02

Bestandsaufnahme: Datenschutzrecht für Notare

03

Datensicherheit im Notariat

04

Resümee

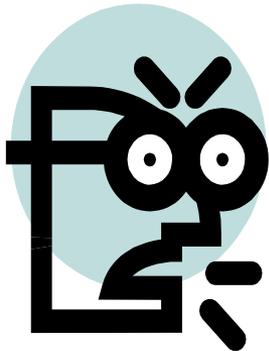
/01

Einführung

Notare und Datenschutz?



Datenschutz, das
unbekannte Wesen



Datenschutz? Betrifft mich
als Notar nicht!



Datenschutz? Als Notar bin ich
zum Datenschutz geboren!

Notare als geborene Datenschützer?



§ 18 BNotO

(1) Der Notar ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm bei Ausübung seines Amtes bekannt geworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [...]

/02

Grundlagen des Datenschutzrechts

Bestandsaufnahme: Quellen

- EU-Datenschutz-RL (95/46/EG)
- BDSG (nicht-öffentliche Stellen und öffentliche Stellen des Bundes)
- Landesdatenschutzgesetze (öffentliche Stellen der Länder)
- EU-Datenschutz(-Grund)VO (Vorschlag vom 25.01.2012, KOM(2012)11 endg.)

Bestandsaufnahme: Anwendungsbereich

- Notare als öffentliche Stellen
- Anwendbarkeit der Landesdatenschutzgesetze
- Subsidiaritätsgrundsatz

Subsidiaritätsgrundsatz

§ 2 Abs. 4 SächsDSG

(4) **Soweit** besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes den Schutz personenbezogener Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor.

- Verdrängung bei Tatbestandskongruenz
- § 18 BNotO als bereichsspezifische, das allgemeine Datenschutzrecht insgesamt verdrängende spezialgesetzliche Regelung?

Begriffsbestimmungen: Datenverarbeitung

- **Erheben:** Beschaffen von Daten
- **Verarbeiten** i.e.S.: Speichern, Verändern, Sperren, Übermitteln, Löschen
- **Nutzen:** jede Verwendung von Daten, soweit sie nicht Verarbeitung ist

Zulässigkeit der Datenverarbeitung

§ 4 SächsDSG

- (1) Die Verarbeitung personenbezogener Daten ist nur zulässig,
1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
 2. soweit der Betroffene eingewilligt hat.
- [...]
- (4) Die Einwilligung und die Hinweise bedürfen der Schriftform, soweit nicht im Einzelfall wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Regelungsbereiche: materielles Datenschutzrecht

- Zulässigkeit der Erhebung/Verarbeitung/Nutzung
 - **Einwilligungsgrundsatz** (in der Regel schriftlich)
 - Erlaubnis oder Anordnung durch Rechtsvorschrift
- Zulässigkeit der Übermittlung (§ 14-17 SächsDSG)
- Auskunft- und Informationspflichten (§ 18 SächsDSG)
- Löschung, Sperrung (§ 20, 21 SächsDSG)
- Berichtigung (§ 19 SächsDSG)
- Widerspruchsrecht (§ 22 SächsDSG)
- Schadensersatz (§ 23 SächsDSG)
- **Grundsatz der Datensparsamkeit**



Beispiel: Recht auf Löschung/Widerspruch (1)

§ 5 SächsDSG

Rechte des Betroffenen

- (1) Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf
1. Auskunft über die zu seiner Person gespeicherten Daten (§ 18),
 2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§ § 19 bis 21),
 3. Widerspruch gegen die Verarbeitung seiner Daten (§ 22),
- [...]

Beispiel: Recht auf Löschung/Widerspruch (2)

§ 20 SächsDSG

Löschung

- 
- (1) Personenbezogene Daten sind zu löschen, wenn,
1. ihre Speicherung unzulässig ist oder
 2. ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist..
- [...]
- (4) Die Löschung unterbleibt, wenn
1. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden,
 2. sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist
- oder
3. ihr durch Rechtsvorschriften bestimmte Aufbewahrungsfristen entgegenstehen

Beispiel: Recht auf Löschung/Widerspruch (3)

§ 22 SächsDSG Widerspruchsrecht

- (1) Der Betroffene kann im Einzelfall gegenüber der Daten verarbeitenden Stelle der beabsichtigten oder weiteren Verarbeitung seiner Daten widersprechen.
- (2) Die Verarbeitung der Daten unterbleibt dann insoweit, als dies zur Wahrung der vom Betroffenen geltend gemachten schutzwürdigen, sich aus einer besonderen persönlichen Situation ergebenden Gründe erforderlich ist und diesen Gründen Vorrang gegenüber den Interessen der Daten verarbeitenden Stelle an einer beabsichtigten oder weiteren Verarbeitung der betroffenen Daten einzuräumen ist; dies gilt nicht, wenn dem Unterbleiben der Verarbeitung eine Rechtsvorschrift entgegensteht.

Weitere Regelungsbereiche des Datenschutzrechts

- Aufsicht
 - parallele Aufsicht durch Dienstaufsicht und Landesdatenschutzbeauftragten
 - Aufsicht des LDSB erstreckt sich auch auf bereichsspezifisches Datenschutzrecht
- Behördlicher/betrieblicher Datenschutzbeauftragter
 - Unterschiedliche Länderregelungen vs. EU-DatenschutzVO-E
 - Muss-/Kann-Vorschrift/Dispens für Notare
 - Bestellung eines gemeinsamen DSB für mehrere Stellen
 - Aufgaben:
 - Beraten und Koordinieren, in gewissem Maße aber auch Kontrollieren
 - Freigabe automatisierter Verfahren
 - Verzeichnisverzeichnis



03 | Datensicherheit im Notariat



**§ 18 BNotO:
Der Notar ist zur Verschwiegenheit
verpflichtet.**



**§ 5 Abs. 3 S. 1 DONot:
Die Unterlagen sind in der Geschäftsstelle
zu führen.**



Technisch-organisatorische Maßnahmen

Anlage zu § 9 Satz 1 BDSG

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 genutzt 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.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.



04 | Resümee

Vielen Dank für Ihre
Aufmerksamkeit!

Marius Klingler
Bundesnotarkammer

Mohrenstraße 34
10117 Berlin
Deutschland
Telefon: +49 30 383866-0
Fax: +49 30 383866-66
m.klingler@bnotk.de
www.bnotk.de