Projective Expert Group

Sachverständigenbüro & IT-Beratungshaus

Version v002

Sachverständigentag 2018

EU-Datenschutzgrundverordnung und IT-Sicherheit im Sachverständigenbüro

24. Oktober 2018

Dr. Frank Sarre

Öffentlich bestellter und vereidigter Sachverständiger für
Systeme und Anwendungen der Informationsverarbeitung
(IHK für München und Oberbayern)

Gliederung des Vortrags

1. **Einleitung**

2. **Rechtliche Grundlagen** (Datenschutz und Informationssicherheit)

3. Relevante **Themen** für Sachverständige
   und konkrete **Handlungsempfehlungen**

4. **Diskussion**

Einleitung (1)

Am 25. Mai 2018 sind in Kraft getreten:

- **EU-DSGVO**
- **BDSG neu,** das die EU-Regelungen ergänzt und verschärft
- **BayDSG (Bayerisches Datenschutzrecht)**

→ **Datenschutz wird immer wichtiger**

→ **Spielräume** in Sachen Informationssicherheit und Datenschutz **schrumpfen**

→ Die neuen Regelungen **gelten auch für Sachverständigenbüros** jeder Größe!

Einleitung (2)

Verantwortlichkeiten

Chefsache!

– Die **Geschäftsleitung** eines Sachverständigenbüros ist für die Themenbereiche Informationssicherheit und Datenschutz **verantwortlich**

→ Entsprechende **Maßnahmen** müssen geplant, umgesetzt und (ständig) kontrolliert werden

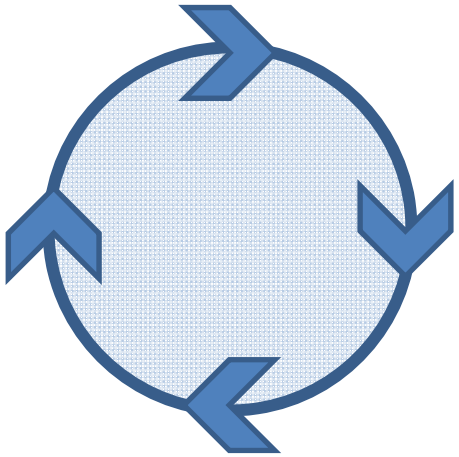
→ Sachverständigenbüros müssen aufgrund ihrer geringen Unternehmensgröße **viel Energie** aufwenden, um allen Anforderungen hinsichtlich Informationssicherheit und Datenschutz gerecht zu werden

Einleitung (3)

Informationssicherheit und **Datenschutz** als **kontinuierlicher Prozess**

Initiale Schutzbedarfs- und Risikoanalyse

Planung der Informationssicherheit und des Datenschutzes



Umsetzung der Maßnahmen

Prüfung der Maßnahmen

Verbesserung der Maßnahmen

Einleitung (4)

Vorteile für Verantwortliche

- **Rechtliche Konformität** zum Datenschutz / Vermeidung von Strafen
- **Ausfallsicherheit** der eigenen IT-Infrastruktur und **Wiederherstellbarkeit** der Arbeitsfähigkeit nach Notfällen
- **Angriffssicherheit** und **Schutz vor Datenklau / -missbrauch / -verlust**
- Daten und Anwendungen werden im Rahmen des kontinuierlichen Prozesses i.a.R. **„aufgeräumt“** (→ Reinigungseffekt!)

Einleitung (5)

Datenarten im Sachverständigenbüro

- Buchhaltungsdaten und sonstige wirtschaftliche Kennzahlen des SV-Büros
- (Personenbezogene) Daten der Angestellten
- Eigenes Know-how
  (Vorlagen, Mustergutachten, Softwarekonfigurationen, Werkzeuge, Zugangsdaten, …)
- Nutzerspuren (Internetzugriffe, Telefonate, Protokolle von Web-Shops, etc.)
- Ggf. Daten aus Videoaufzeichnungen
- Kunden- und Lieferantendaten
- Daten aus Gerichtsfällen und Parteigutachten
- Sonstige vertrauliche Daten

→ **Alle Daten** haben unterschiedliche Eigenschaften und **erfordern in aller Regel unterschiedliche Maßnahmen** in Bezug auf Informationssicherheit und Datenschutz

Einleitung (6)

Personenbezogene Daten im Sachverständigenbüro

- Adressdaten aller Art (Namen, Telekommunikationsdaten, etc.)
- Vertragsdaten
- Beschäftigtendaten
- Daten, die im Rahmen von Gutachten verarbeitet werden
  (darunter könnten u.U. auch besondere Kategorien personenbezogener Daten sein)
- Zugangsdaten zu IT-Systemen
- Nutzungs- und Verbindungsdaten (Internet, E-Mail, Telefon, etc.)
- Telekommunikationsinhalte
- Nutzungsdaten der eigenen Internetseiten

Grundzüge des aktualisierten Datenschutzrechts

- Die **Rechte der Betroffenen** sind gestärkt worden
- Die **Dokumentations- und Meldepflichten** wurden stark ausgeweitet
- **Informationspflichten** gegenüber den Betroffenen sind gestiegen
- **Risikobetrachtung** für personenbezogene Daten erforderlich, damit ein „angemessenes“ Schutzniveau sichergestellt werden kann
- Es drohen wesentlich höhere **Bußgelder** (früher max. 300.000 EUR)

Wichtige rechtliche Themen (1)

- Geldbußen
  - Gegebenenfalls bis zu 20 Mio EUR oder 4% des weltweiten Jahresumsatzes des vorausgegangenen Jahres
- Datenschutzbeauftragter
  - Zwingend zu bestellen, wenn mindestens 10 Personen personenbezogene Daten verarbeiten
  - Auch zwingend zu bestellen, wenn mit Daten über strafrechtliche Verurteilungen gearbeitet wird und diese Tätigkeiten dem Kerngeschäft des Sachverständigenbüros zuzurechnen sind
- Verzeichnis der Verarbeitungstätigkeiten
  - Muss der Aufsichtsbehörde auf Verlangen vorgelegt werden
  - Ist nicht mehr zu veröffentlichen
- Informations- und Auskunftspflichten

Wichtige rechtliche Themen (2)

- Löschen von Daten
  - Wenn der Verarbeitungsgrund nicht mehr besteht, sind die betroffenen Daten zu löschen
  - Auf Verlangen des Betroffenen sind seine eigenen Daten zu löschen, wenn nicht gesetzliche Aufbewahrungsfristen etwas anderes fordern
- Gesetzliche Aufbewahrungspflichten
  - U.a. aus dem Geldwäschegesetz (GwG), der Abgabenordnung (AO), etc.
  - Vorrang vor dem „Recht auf Vergessen“
  - Sehr häufig 5 oder 10 Jahre
- Auftragsverarbeitung
  - Liegt nur vor, wenn die Weisungsabhängigkeit gegeben ist
  - Es muss ein Vertrag geschlossen werden bezüglich Weisungsrecht, Tätigkeiten, Vertraulichkeit und Handhabung der Daten nach Vertragsende
- Zweckbindung
  - Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben worden sind

Wichtige rechtliche Themen (3)

- Datenschutzverletzungen & Management von datenschutzrelevanten Vorfällen
- Videoüberwachung
- Datenschutzfolgeabschätzung
- Unterweisung von beschäftigten Mitarbeitern
- Verpflichtung der Beschäftigten auf das Datengeheimnis

Erlaubnistatbestände für die Verarbeitung personenbezogener Daten

- (Informierte) **Einwilligung** (Art. 6 Abs. 1 lit. a)
- Erfüllung eines **Vertrags** und Vertragsanbahnung (Art. 6 Abs. 1 lit. b)
- Erfüllung einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c)
- Schutz **lebenswichtiger Interessen** der betroffenen Person (Art. 6 Abs. 1 lit. d)
- Wahrnehmung einer **Aufgabe im öffentlichen Interesse** (Art. 6 Abs. 1 lit. e)
- **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Art. 6 Abs. 1 lit. f)
- … (siehe DSGVO)

Technische Forderungen der DSGVO

- **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste
- **Anonymisierung, Pseudonymisierung und Verschlüsselung** von personenbezogenen Daten (soweit möglich)
- **Wiederherstellbarkeit** der Daten und Zugänge nach einem Zwischenfall
- Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der Maßnahmen

→ **Risikoanalyse ist hier unerlässlich**

Organisation innerhalb des Sachverständigenbüros (1)

Die **Einhaltung des Datenschutzes muss nachgewiesen** werden können

- Risikoanalyse
- Verzeichnis der Verarbeitungstätigkeiten
- Technische Maßnahmen
- Sensibilisierung und Verpflichtung der Mitarbeiter
- Meldung von Datenpannen
- Einwilligungen
- Auskunftsersuchen von Betroffenen

Organisation innerhalb des Sachverständigenbüros (2)

Arbeitsrichtlinien

- Passwort-Policy
- Umgang mit mobilen Datenträgern
- Nutzung und Installation von Software
- Mobile Device Policy
- Vernichtung von Papier und Datenträgern
- Meldepflichten im Falle von Notfällen / Problemfällen / Datenpannen
- E-Mail- und Telefon-Policy
- Home Office Policy
- …

Organisation innerhalb des Sachverständigenbüros (3)

- **Verschlüsselung** von Daten
- **Anonymisierung** und **Pseudonymisierung** von Daten
- **Redundanz** zur Sicherung der Verfügbarkeit von Anwendungen und Daten
- Rasche **Wiederherstellung** nach Störfällen
- Regelmäßige **Kontrolle**

Internet-Auftritt des Sachverständigen

- **Webserver-Logfiles** → IP-Adressen anonymisiert?
- **Kontaktformulare** → Verschlüsselung per https!
- **Cookies** → Hinweisplicht!
- **Analysetools / Plug-ins** → IP-Adressen anonymisiert?
- **Social-Media-Plugins** → Datenschutzkonform eingebunden?
- **Newsletter** → Verschlüsselung personenbezogener Daten!
- **Datenschutzhinweis** → Rechtliche Rahmenbedingungen!
- **Nutzung eines Providers** → Vertrag zur Auftragsdatenverarbeitung!
- **Impressum** → Rechtliche Rahmenbedingungen!

IT-Sicherheit

Typische Gefährdungen

- Höhere Gewalt (z.B. Sturm, Feuer, Wasser, Blitzschlag)
- Organisatorische Mängel (z.B. unterlassene Updates)
- Menschliche Fehlhandlungen (z.B. versehentliche Datenlöschung)
- Technisches Versagen (z.B. Ausfall einer Festplatte)
- Vorsätzliche Handlungen (z.B. „Klauen“ von Daten und Source Code)

Präventionsmaßnahmen - Beispiele (1)

- Gebäude- und Raumzugangskontrolle
- Einbruchmeldeanlage
- Videoüberwachung
- Brandschutz
- Benutzer- und Berechtigungsmanagement
- Passwortmanagement
- Sichere Archivierung

Präventionsmaßnahmen - Beispiele (2)

- Nutzungsrichtlinien für mobile Endgeräte
- Verwendungsrichtlinien für Cloud-Dienste
- Besucherregelungen
- Notfallmanagement
- Passwortrichtlinien
- Löschen / Vernichten von personenbezogenen Daten auf geleaseten oder gemieteten IT-Geräten, die zurückgegeben werden müssen
- Kein Arbeiten im öffentlichen Raum (Flughafen, Bahn, etc.) oder nur unter bestimmten Vorkehrungen
- „Richtiges“ Löschen von nicht mehr benötigten Daten
- Sensibilisierung der Mitarbeiter

Präventionsmaßnahmen - Beispiele (3)

- Patch Management für Betriebssysteme und Anwendungen
- Anti-Malware-/ Virenschutz-Lösungen
- Backup- und Recovery-Lösungen
- Redundante Systeme und Infrastruktur
- Protokollierung kritischer Tätigkeiten (z.B. ändern von personenbezogenen Daten)
- Anonymisierung und Pseudonymisierung personenbezogener Daten
- Umfangreiche Verschlüsselung von Daten auf Datenträgern unterschiedlichster Art
- Einsatz der VPN-Technologie
- Firewall(s)
- Mobile Device Management
- Sperren von Schnittstellen (USB etc.)
- Protokollierung von Benutzeraktivitäten

Verschlüsselung

Daten müssen – wo immer möglich – verschlüsselt werden:

- Festplatten / SSDs in Computern
- USB-Sticks
- Smartphones
- Cloudspeicher
- E-Mail-Texte und -Anhänge
- Transportwege
  (Browser ⇔ fremde Webserver,
  Datenübertragung über fremde Computernetze)

Zusammenfassung

- Informationssicherheit und Datenschutz sind **Chefsache**!
- In jedem Sachverständigenbüro sind auch die **formalen Anforderungen** des Datenschutzes zu erfüllen.
- Der **Internetauftritt** des Sachverständigenbüros muss an die neuen Datenschutzvorschriften angepasst werden.
- Technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der IT-Sicherheit müssen **aufeinander abgestimmt** sein und zusammenspielen (Konzept „aus einem Guss“).
- Viel gewonnen ist schon durch:
  - Verschlüsselung
  - Backup- und Recovery
  - Passwortrichtlinien
  - Redundante Systeme und Infrastruktur
- Die **regelmäßige Kontrolle** aller Maßnahmen ist essenziell!

Literatur und weiterführende Informationen

Behörde / Verein / Organisation	Internet-URL
Bayerisches Landesamt für Datenschutzaufsicht	https://lda.bayern.de/ Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine Broschüre 2017, Verlag C.H.BECK, ISBN 978-3-406-71662-1, Preis: 5,50 EUR
Bayerisches Staatsministerium des Inneren und für Integration	www.dsgvo-verstehen.bayern.de
bitcom	https://www.bitkom.org/
BSI	https://www.bsi.bund.de
BVS	Wirwohl, V.: Die Umsetzung der Datenschutz-Grundverordnung durch Sachverständige: Was ist zu beachten? DS 6/2018, S. 162-165 Sonderbrief, Heft April 2018
Davit	https://www.davit.de
Deutschland sicher im Netz e.V.	https://www.sicher-im-netz.de/
IHK	www.ihk-muenchen.de/dsgvo
Immobilienverband IVD	Das neue Datenschutzrecht für die Praxis der Immobilienmakler und Sachverständigen, Broschüre März 2018 (nur für IVD-Mitglieder)
Sicherheit in der Wirtschaft	https://www.sicher-im-netz.de/it-sicherheit-der-wirtschaft-0

Fragen …. ?

Kontaktdaten

Dr. Frank Sarre

- Öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung
- Lehrbeauftragter der LMU München, Fachbereich Informatik

Projective Expert Group GmbH
Lindwurmstr. 149
80337 München

Telefon 089 / 18 92 37 -01
Mobil 0172 / 8 215 295
Email: frank.sarre@projective.de