Koblenz, den 28. März 2019

Nach Inkrafttreten der DSGVO – Geänderte Anforderungen an technische und organisatorische Datensicherheit

Dr. Paul H. Klickermann

Rechtsanwalt

Fachanwalt für Urheber- und Medienrecht

Lehrbeauftragter der Universität Mainz

Alexander Dörsam

Geschäftsführer der Antago GmbH (Bensheim)

Alexander Metzler

Rechtsanwalt

Datensicherheit

- Summe von erforderlichen Maßnahmen, um Ablauf der Datenverarbeitung sicherzustellen (Art. 32 DSGVO).
- Erforderlich sind Maßnahmen nur, wenn Aufwand im angemessenen Verhältnis zum Schutzzweck steht.
- Hierzu gehört u. a. Sicherung von Hard- und Software sowie Schutz der Daten vor Verlust, Beschädigung und Missbrauch.
- Sowohl der Verantwortliche als auch Auftragsverarbeiter sind zur Datensicherheit verpflichtet.

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Personenbezogene Daten können ohne Hinzuziehung zusätzlicher Informationen nicht einer betroffenen Person zugeordnet werden.
- Zusätzliche Informationen müssen gesondert aufbewahrt werden.
- Verschlüsselungsverfahren muss bewirken, dass der Zugang zu personenbezogene Daten, die nicht hierzu befugt sind, unmöglich gemacht wird.
- Es werden keine Vorgaben zur Art der Verschlüsselung gemacht.

Vertraulichkeit (1)
(Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  - Gebäude- und Raumsicherung.
  - Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder.
  - Server, Netzwerktechnik in verschließbaren Serverschranken.
  - Organisatorische Maßnahmen (z. B. Dienstanweisung).
- Zugangskontrolle
  - Unbefugte Verhinderung der Nutzung von Anlagen.
  - z. B. Passwort, Benutzerkennung mit Passwort für Betriebssysteme, Bildschirmschoner mit Passwort.

Vertraulichkeit (2)
(Art. 32 Abs. 1 lit. b DSGVO)

- **Zugriffskontrolle**
  - Benutzung eines Datenverarbeitungssystems nur durch den Berechtigten.
  - Personenbezogene Daten dürfen nach Verarbeitung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
  - Gewährleistung durch geeignete Berechtigungskonzepte
  - Kontrollmechanismen und Verantwortliche sind zu definieren.
- **Trennungskontrolle**
  - Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobene Daten (z. B. physikalisch).

Integrität
(Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**
  - Personenbezogene Daten dürfen bei Übertragung oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert oder verändert.
  - Feststellung, an welcher Stelle die elektronische Übermittlung der Daten vorgesehen ist.
  - Gewährleistung der Vertraulichkeit der elektronischen Datenübertragung durch Verschlüsselungstechniken.
- **Eingabe- und Verarbeitungskontrolle**
  - Nachträgliche Überprüfung, ob und von wem personenbezogene Daten in Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.
  - Eingabekontrolle durch Protokollierung auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall).
  - Klärung, welche Daten protokolliert werden und wer Zugriff auf die Protokolle hat; Aufbewahrung und Löschung der Protokolle.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**
  - Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
  - z. B. unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz und Plattenspiegelungen.
- **Belastbarkeitskontrolle**
  - Schutz der Systeme vor versehentlicher und absichtlich herbeigeführter Überlastung (etwa durch sog. „Denial of Service“-Attacken).

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (1) (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)

- **Prüfkontrolle**
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer IT-Sicherheitsmaßnahmen.
  - Bei Wirksamkeit wird auf nationale Standards (z. B. BSI-Grundschutzstandards) zurückgegriffen:
    - Managementsysteme für Informationssicherheit
    - IT-Grundschutz-Vorgehensweise
    - Risikoanalyse auf der Basis von IT-Grundschutz
    - Notfallmanagement
  - Datenschutzfreundliche Voreinstellungen sind zu beachten.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (2) (Art. 32 Abs. 1 lit. d, Art. 28 DSGVO)

- **Auftragskontrolle**
  - Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort und auch per Fernwartung.
  - Bei Auftragsverarbeitung sind folgende Maßnahmen zu beachten:
    - Vorherige Prüfung der Sicherheitsmaßnahmen des Auftragnehmers
    - Auswahl und Vereinbarung mit Auftragnehmer
    - Schriftlich Weisung an den Auftragnehmer
    - Im Falle der Bestellpflicht Datenschutzbeauftragter durch Auftragnehmer zu benennen
    - Regelung des Einsatzes weiterer Subunternehmer
    - Vereinbarung wirksamer Kontrollrechte gegenüber Auftragnehmer
    - Sicherstellung der Vernichtung der Daten nach Ende des Auftrags

Vielen Dank für Ihre Aufmerksamkeit!

Dr. iur. Paul Klickermann
Rechtsanwalt

FROMM
Kanzlei für Unternehmens- und Steuerrecht
August-Thyssen-Straße 27
56070 Koblenz
Fon: 0261/98183-15
Fax: 0261/98181-11
info@fromm-koblenz.de
www.fromm-koblenz.de

„Passwort“ ist kein Passwort

Wie sicher ist das folgende Passwort?

ji32k7au4a83

- Stark auf den ersten Blick, aber:
- Keine zufällige Buchstaben-Zahlen-Kombination, sondern die Transliteration von Mandarin in lateinische Buchstaben
- Bedeutet “My Password”
- Bereits über 100 Mal von Leaks betroffen

den Hygieneregeln. „Mit dem Hände-
waschen können wir Krankheiten

Top 10 bei Passwörtern
in Deutschland

	Wörter	Wörter oder Zahlen
1	hallo	123456
2	passwort	123456789
3	hallo123	12345
4	schalke04	hallo
5	passwort1	1234
6	qwertz	passwort
7	arschloch	12345678
8	schatz	hallo123
9	hallo1	schalke04
10	ficken	1234567

HANDELSBLATT Quelle: HPI

Gefunden über Prof. Keber –
www.twitter.com/datenreiserecht

Passwortsicherheit

- Ein starkes Passwort ist kein komplexes, sondern ein langes:
  - Mind. 8 – 10 Zeichen, Groß- und Kleinschreibung, Sonderzeichen, bei WLAN sogar mind. 20 Zeichen für WPA2 (WPA3 ist angekündigt)
  - Denken Sie sich einen Satz aus und nehmen Sie den ersten (zweiten oder dritten) Buchstaben eines jeden Wortes, z.B. Datenschutz geht jeden an und ist auch gar nicht schwer! – Dsgjauiagns! -> Dsgj4&1agnS!
  - Alternativ: 5 oder mehr (Phantasie-) Worte durch Leerzeichen getrennt
  - Grundsatz: Je wichtiger das Passwort, desto länger sollte es sein

- Lügen Sie bei Sicherheitsfragen, diese sind anfällig für Social Engineering!

- Prüfen Sie, ob Ihre persönliche Daten wie E-Mail-Adresse und Passwörter bereits veröffentlicht sind
  - Have I been pwned? -. https://haveibeenpwned.com/
  - Identity Leak Checker des Hasso-Plattner-Insitut der Universität Potsdam - https://sec.hpi.de/ilc/

Best Practices für Unternehmen

- Passwortrichtlinien einführen
  - Zwang zu regelmäßigen Änderungen führt meist dazu, dass dasselbe Passwort nur leicht modifiziert wird
  - Fehlgeschlagene Anmeldeversuche protokollieren
  - Wo möglich, 2-Faktor-Authentifizierung nutzen
- Passwörter keinesfalls im Klartext speichern, sondern immer als Hash mit Salt und Pepper
- Voreingestellte Passwörter ändern
- Passwörter nicht doppelt verwenden, besonders nicht für berufliche und private Zwecke
  - Passwort Safes wie KeePass (Open Source) erleichtern das Management

Rechtemanagement

- Zwei Grundprinzipien:
  - Das schwächste Glied in der Kette ist immer das anfälligste
  - Der größte Unsicherheitsfaktor ist der Mensch vor der Maschine

- Berechtigungskonzept festlegen in drei Schritten
  - Was? - Alle Nutzer, Geräte und Software erfassen:
    - Mitarbeiterlisten, Projektlisten, Organigramme, Hardware- und Softwarelisten können helfen
  - Wer? - Identitäten abbilden:
    - Alle Personen, Geräte und Software mit Zugriff auf Datenbestand müssen eindeutig und zuverlässig identifizierbar sein
  - Wozu? - Zugriffsrechte festlegen:
    - Keine Berechtigung; Daten nur lesen; Daten erfassen / erstellen; Daten bearbeiten; Daten löschen; Vollzugriff

Datensicherung / Zugang zu Daten

- Ziel: Gewährleistung von CIA – Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit)

- Regelmäßig Datensicherungen vornehmen
  - Legen Sie Verantwortlichkeiten fest
  - Backups redundant erstellen und bereit halten
  - Festplatten verschlüsseln
- Backups nicht mit nach Hause nehmen! Selbstgeschaffenes Risiko, das sich leicht vermeiden lässt!

- Serverräume geschlossen halten, Zugang für Mitarbeiter und Dienstleister begrenzen
- Server nicht offen stehen lassen, sondern in einem gesicherten Schrank gegen unbefugte Zugriffe schützen

Vielen Dank für Ihre Aufmerksamkeit!

Alexander Metzler
Rechtsanwalt

FROMM
Kanzlei für Unternehmens- und Steuerrecht
August-Thyssen-Straße 27
56070 Koblenz
Fon: 0261/98183-15
Fax: 0261/98181-11
info@fromm-koblenz.de
www.fromm-koblenz.de

Folgeveranstaltungen:

09. Mai 2019

Nach Inkrafttreten der DSGVO – Neue Herausforderungen in der Zusammenarbeit mit anderen Unternehmen

27 Juni 2019 – „*Wissen. Werte. Weine*.“ im Schlossgut Diel

Nach Inkrafttreten der DSGVO – Datenschutzaudit: Stellen Sie Ihr Unternehmen auf den Prüfstand

Externer Referent: Christian Heller, Geschäftsführer Recht bei Klosterfrau Melissengeist, zum Thema „Compliance“