150 Tage DSGVO
Umsetzungserfahrungen in der Praxis mit KMU

Jens Bitter

16.10.2018

Agenda

- DSGVO – Anspruch und Wirklichkeit
- Pragmatische (?!) Umsetzung in KMU‘s
- Top 10 Umsetzungsfehler
- Anforderungen an DSGVO-konforme Anwendungen / IT

Anmerkung

- Der Vortrag erhebt weder den Anspruch die gültige Gesetzeslage noch die nötigen Umsetzungsaktivitäten umfassend und vollständig darzustellen.
- Die Darstellung basiert auf den Erfahrungen des Autors bei der Etablierung von Datenschutzprozessen und ist hier fokussiert auf kleine und mittlere Unternehmen (KMU).

Was schützt der Datenschutz ?

- Personenbezogene Daten
  - Alles, womit sich Personen (Betroffene) identifizieren lassen
    - z.B.: Name, Anschrift, Telefonnr., eMail, Bankverbindung
- Verarbeitungsumfang
  - Jedweder Umgang mit personenbezogenen Daten, von der Erhebung bis zur Löschung
- Verarbeitung
  - Jede Verarbeitung personenbezogener Daten ist verboten, es sei denn der Betroffene oder eine Rechtsvorschrift erlauben diesen Vorgang
- Prinzipien
  - Datenminimierung, **geregelte Verarbeitung**

Rechte der Betroffenen

- Auskunft bzgl. verarbeiteter Daten (Art. 15 DSGVO)
- Berichtigung (Art. 16 DSGVO)
- Löschung / Einschränkung (Art. 17/18 DSGVO)
- Bereitstellung (Art. 20 DSGVO)
- Beschwerde (Art. 77 DSGVO)
  - bei der zuständigen Aufsichtsbehörde
- Widerruf erteilter Einwilligungen (Art. 7 III DSGVO)
- Widerspruch zukünftiger Verarbeitung (Art. 21 DSGVO)

Status Quo KMU (t – 150, t heute ?)

- Missachtung bestehender Gesetzeslage (BDSG)
  - Pro forma DS-Erklärungen, Verzeichnisse
  - Lediglich ad-hoc (bei Anfragen)
  - Rudimentäre Umsetzung, kein lebendiger Prozess
  - „Papier ist geduldig“
- Keine Aktivität, sofern nicht dem Geschäftszweck förderlich

Erforderlicher Datenschutzprozess

- Datenschutzmanagement
  - Festschreibung, Regeln und Richtlinien
  - Risikoanalyse, Technisch-Organisatorische Maßnahmen, Verarbeitungsverzeichnis
  - Auftragsverarbeitung (inkl. Prüfung)
  - Erklärungen (Web, Geschäftsräume, Verträge)
  - Auskunftsanfragen (von Betroffenen, LDSB)
  - Meldungen (bei meldepflichtigem Vorfall an LDSB)
  - Prozess- und Durchführungsdokumentation

- Management von Sicherheits-/Datenschutzvorfällen
  - Reaktionsplan

Welche Daten werden verarbeitet ?

- Bestandsdaten
  - Name, Anschrift
- Kontaktdaten
  - Telefonnummer, eMail, Social Media
- Vertragsdaten
  - Angebot, Bestellung, Vertragsgegenstand, Reklamation
- Zahlungsdaten
  - Bankverbindung, Zahlungshistorie

DSGVO – rechtlicher Rahmen

- Interessenten / Kunden **Fokus KMU**
  - Auftragsanbahnung / -abwicklung / -beendigung
    - Rechtsvorschrift DSGVO Art. 6, I b)
  - Werbung bestehender Kunden
    - Rechtsvorschrift DSGVO Art. 6, I f)
  - Werbung neuer Kunden
    - Rechtsvorschrift DSGVO Art. 6, I a) – Einwilligung !
- Mitarbeiter / Vertragspartner
  - Verpflichtungs- und Vertraulichkeitserklärung
    - Rechtsvorschrift DSGVO Art. 5, I sowie BDSG §26
- (Sub-) Dienstleister
  - Vertrag zur Auftragsverarbeitung
    - Rechtsvorschrift DSGVO Art. 28 in Verb. mit Art. 32

Top 10 Fails

- Nutzung Drag & Drop Tools, Generatoren
  - DS-Erklärungen, Verarbeitungsverzeichnis
- Nicht funktionaler (Incident) Response Prozess
  - Vorfälle, Kundenanfragen nach DSGVO
- Auftragsdatenverarbeitung
  - Prozessmängel, Haftungsausschlüsse, unzulängliche TOM‘s, veraltete Unterlagen
- Sourcing
  - Juristen, DS-Berater ohne Umsetzungserfahrung

DSGVO-konforme IT / Anwendungen

- Erfassung Geschäftsprozesse- / IT-Verfahren
  - Verarbeitungsverzeichnis (sinnvollerweise mit internen Ergänzungen zu Schnittstellen)
  - Gut standardisierbar, aber trotzdem wichtig, intelligente Fragen im Interview mit GF zu stellen, um reale Verhältnisse korrekt zu erfassen
- Risikomanagement
- Sicherheitsmaßnahmen (TOM‘s)
- Spezifische Anforderungen an Anwendungen

- Spannungsfeld: Anerkannte Regeln der Technik, Stand der Technik, Stand der Wissenschaft und Technik

Sicherheitsmaßnahmen (TOM)

- Organisation der IT-Nutzung
  - Zentrale Benutzerverwaltung (Identifikation und Authentisierung)
  - Zentrale Rechteverwaltung (Authorisierung), technisch nur soweit sinnvoll und möglich
  - Zentrale System- und Netzwerkverwaltung
  - Protokollierung von Konfigurationsänderungen und Datenzugriff
  - Notfallplan zur Sicherstellung Verfügbarkeit
  - Identifizierung Anwendungssupport (durch Dienstleister – AV !)
    - Protokollierung aller Supportvorgänge (Zeitpunkt (Datum / Uhrzeit), Name des Supporters, Firma, Kurzbeschreibung Problem)

- Nutzung von Firmencomputer / Anwendungen
  - Sperrung der Arbeitsstation bei (auch kurzer) Abwesenheit
    - besonders bei öffentlich zugänglichen Systemen
  - Verwendung sicherer Passwörter
    - keine Notiz unter der Tastatur o.ä.
  - Keine Installation / Nutzung nicht freigegebener Anwendungen
  - Anti-Virenschutz
  - Regelmäßige Windows-Updates

- Umgang mit „sensitiven“ Informationen (Daten im Sinne DSGVO + Firmengeheimnisse)
  - Keine Verwendung außerhalb hierfür vorgesehener Anwendungen
  - Keine Auswertung / Speicherung / Ausdruck nicht benötigter Datensätze
  - Entsorgung von Ausdrucken in gesondertem Sammelbehälter zur geregelten Vernichtung
  - Kein inhaltlich unverschlüsselter Versand von Massendatensätzen (z.B. eMail, Datenträger)

DS-spezifische Anforderungen an Anwendungen

- Nachvollziehbarkeit im Customer Data Management
  - Stammdatenänderungen (DSGVO Art. 16 – 18)
  - Beauskunftung (DSGVO Art. 15, 20)
  - Widerruf, Widerspruch (DSGVO Art. 7, 21)
- Integrität in Anwendungen / Datenbanken
  - Umsetzung Datensperren für best. Zwecke (s.o.)
  - Ggf. Ano-/Pseudo-nymisierung für Auswertungen
- Systemisch erzwungene Löschfristen (Festlegung in DSMS)
- (DS-) Datenminimierung – Kosten / Nutzen - Betrachtung
- Datenexport Schnittstellen

„Erfassen, was zur Geschäftsabwicklung gebraucht wird, aber ohne Plan nicht auf Zukünftiges spekulieren“

FRAGEN?

Dipl.-Ing. Jens Bitter, JB CyberSecurity

IT Governance, IT Risk & IT Security Management Consultant
Interimsmanagement / Information Security Officer
Betrieblicher Datenschutzbeauftragter (TueV Nord)
CISM, CISSP, CRISC, ISO22301 & ISO27001 Lead Auditor

Mobile: *0151-40742514*
eMail: *jens@istdasbitter.de*

XING: *https://www.xing.com/profile/Jens_Bitter*