Datenschutzrechtlich & IT-Sicherheitsanforderungskonformer Prozess zum Erwerb & zur Nutzung von »kollaborativen IT-Tools«

Workshop am 13. 10. 2022
mit der DigitalAgentur Brandenburg
und der Kanzlei Luther

GRUNDLAGE

Wie ist das ZIEL mit dem Einsatz der neuen kollaborations-Software?

Welche DATEN muss ich für dieses Ziel erheben?

Welchen SCHUTZBEDARF haben diese zu verarbeitenden Daten?

① » Pitch Vergabe «

Gesetze: 4. Teil GWB
- Vergabeverordnung (VgV)
- Unterschwellenvergabeordnung (UVgO)

Prinzipien:
- Transparenz
- Wettbewerb
- Gleichbehandlung
- Wirtschaftlichkeitsgebot
- Verhältnismäßigkeit

Ablauf: Planung → Design → Durchführung

Praxisleitfaden zur Durchführung von IT-Beschaffung: UFAB von BMI

Mustervertrage IT-Beschaffung: EVB-IT

② » Pitch Informationssicherheit «

Ziel: „angemessener Schutz von Prozessen, Informationen und informations-verarbeitenden Systemen"

Ziel: Informationssicherheit von Anfang an mitdenken!!!
↳ Sicherheitsziele für Angemessenheit: Vertraulichkeit, Verfügbarkeit, Integrität
↳ Schutzbedarf definiert Angemessenheit!

Regelungen:
- Leitlinie Informationssicherheit
- BSI – Grundschutz
- Informationssicherheits-management der Institution

Vor der Ausschreibung:
- Schutzbedarf der Daten feststellen
- Vorgaben & Anforderungen aus Sicherheits- und Compliance-Vorgaben prüfen & einbeziehen
↳ lassen sich aus Organisationsinternen Dokumenten & BSI-Grundschutz ableiten

Vor der Anwendung:
für jedes Tool muss eigenes/integriertes Sicherheitskonzept vorliegen!

③ » Pitch Datenschutzrecht «

personenbezogene Daten
- identifiziert oder
- identifizierbar

Grundprinzipien
- Rechtmäßigkeit
- Transparenz
- Zweck
- Richtigkeit & Aktualität
- Datenminimierung
- Integrität & Vertraulichkeit

Grundlage der Nutzung
Verbot mit Erlaubnisvorbehalt
↳ Einwilligung
↳ sonstige gesetzliche Regelungen
↳ Auftragsverarbeitung
↳ Der Verantwortliche bleibt in der Haftung!
↳ Der Auftragsdatenverarbeiter hat einige Pflichten
↳ Prüfung durch Siegel möglich, aber nicht alle Siegel vertrauenswürdig

④ » Im Land Brandenburg «

1. Vergabe: Kontrahierungszwang mit dem Zit-BB
2. Informationssicherheit:
   - Leitlinie Informationssicherheit Land Brandenburg: neue Version aktuell in Abstimmung
   - Sicherheitsvorgaben für Landesverwaltungsnetz einzuhalten
3. Datenschutz:
   - Brandenburgisches Datenschutzgesetz
   - Bundesdatenschutzgesetz
   - europaweit geltende Datenschutzgrundverordnung (DSGVO)

© DigitalAgentur Brandenburg
gez. F. Grünewald
CC BY ND 4.0

Inhalte von:
- C. Kuss, D. Amelcenko, N. Langenheim (Luther Rechtsanwaltsgesellschaft mBH)
- R. Seydel, Dr. T. Röchert-Voigt, Dr. F. Grünewald (DigitalAgentur Brandenburg)

» Fallstudie: Einführung der Software MURAL «

Phase A: Marktsichtung & Definition der Anforderungen

Grundlagen klären
↳ Ziel, Art der Daten, Schutzbedarf
↳ Querverbindung zur Informations-sicherheit beachten (TOMs)

Auswahl des Anbieters
① Technische & organisatorische Maßnahmen zum angemessenen Schutz der Daten prüfen
↳ Sitz in der EU?
↳ Zertifikate & Prüfberichte vorhanden?
② Datenminimierung möglich?
↳ privacy by design / default?

(muss für gesamte Kategorie der Auftragsverarbeiter geprüft werden, inklusive Subunternehmen!)

Vorbereitung der Vergabe
③ Eignungskriterien
↳ bieter- und unternehmensbezogen, nicht angebotsbezogen
- Befähigung zur Berufsausübung
- wirtschaftliche & finanzielle Leistungsfähigkeit
- technische & berufliche Leistungsfähigkeit

(beide Kriterien müssen getrennt werden)

④ Zuschlagskriterien
↳ angebots- nicht bieterbezogen!
↳ Leistung vs. Preis = wirtschaftlichstes Angebot
↳ kein genereller Ausschluss bei Hosting in den USA (OLG Karlsruhe, 7.09.22)

(Und müssen bei Vergabe bekannt gegeben werden)

Drittlandtransfer
⑤ Prüfung & Regelung
↳ Verbot mit Erlaubnisvorbehalt
↳ Standardvertragsklauseln } außerhalb der EU
↳ zusätzliche Maßnahmen
- genehmigte Verhaltensregeln
- Zertifizierung
- …

Prüfung der Rechtsgrundlage der Datenverarbeitung
⑥ Rechtmäßigkeit: Einwilligung; Schutz lebenswichtiger Interessen; Vertrag oder rechtliche Verpflichtung; öffentliches Interesse

⑦ Zweck & Erforderlichkeit
↳ Welche Datenkategorien?
↳ Welche Verarbeitungstätigkeiten?
↳ Datenerhebung / -verwaltung / -bearbeitung
↳ Warum? → Zweck + Erforderlichkeit für Zweckprüfung
↳ keine nachträgliche Zweckänderung!

Datenspeicherung und -löschung
⑧ Speicherdauer muss insbesondere bei Backup-Lösungen geprüft werden!
↳ Achtung: Drittlandtransfer insbesondere bei Cloud-Lösungen beachten
⑨ Aufbewahrungsfristen & Löschkonzept prüfen

Auftragsverarbeitungsvertrag
⑩ Art, Zweck & Umfang der Datenverarbeitung
⑪ Pflichten des Auftragsverarbeiters:
- Wahrung Vertraulichkeit der Daten
- Mitwirkungs- & Meldepflichten
- …

Phase B: Ausschreibung & Vergabe

⑫ **Vergabeunterlagen**
- Anschreiben
- Verfahrensbriefe
- Leistungsbeschreibung
- Vertrags-/Ausführungsbedingungen (insb. Auftragsverarbeitungsvertrag)

§ 128 GWB
+ umweltbezogene Belange
+ Schutz Vertraulichkeit von Informationen
+ …

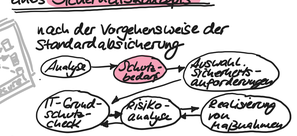
⑬ **Bereitstellung** § 41 VgV, § 29 UVgO
- Veröffentlichung finaler Fassung in elektronischer Form
- Vertrags- und Ausführungsbedingungen müssen auch öffentlich sein!

⑭ **Weitere Schritte im Vergabeverfahren**
- ggf. Bewerbungs- und Prüfungsphase im Teilnahmewettbewerb
- Angebotsphase
- ggf. Verhandlungen
- Prüfung & Wertung der finalen Angebote
- Zuschlag

Phase C: Einführung

⑮ **Erstellung bzw. Integration eines Sicherheitskonzepts**

nach der Vorgehensweise der Standardabsicherung



↳ Einbeziehung vorhandener Sicherheitskonzeption der Organisation notwendig!

⑯ **Verarbeitungsverzeichnis**
- Verantwortliche:r + Zweck
- Rechtsgrund + Löschfristen
- Kategorien für Daten
  - betroffene Personen
  - welche personenbezogenen Daten
  - Empfänger: Hosting-, Cloud-Anbieter…
- Drittlandübermittlung?
- Beschreibung der technischen & organisatorischen Maßnahmen
  - Verschlüsselung
  - Pseudonymisierung
  - Backup
  - Zugriffskontrollen

⑰ **Prozess für Betroffenenrechte**
- Recht auf Informationen, Löschung, Auskunft, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit
- muss durch Dateninhaber umgesetzt werden … zusammen mit anderen Verantwortlichen

⑱ **Datenschutzfolgeabschätzung**
- Prüfung, ob besonderes Risiko für Recht der Betroffenen
  ↳ Prüfung, ob Datennutzung zulässig
  ↳ z. B. biometrische Zutrittskontrolle, Aufenthaltsdaten, Bewertungsportale, KI, …

⑲ **Aktualisierung der Datenschutzerklärung**
- Verantwortliche
- Rechtsgrundlage & Zweck
- verarbeitete Daten
- Betroffenenrechte
- Cookies
- Analysesoftware
- …

⑳ **Handlungsanweisung & Schulungen der Mitarbeiter**