Datenschutzrechtlich und IT-Sicherheitsanforderungs-konformer Prozess zum Erwerb und zur Nutzung von neuen kollaborativen IT-Tools

Stichworte: Datenschutz, Informationssicherheit, Vergabe, IT, kollaborative Software

#DABB
DigitalAgentur Brandenburg

Stand: 07.12.2022, Entwurf V. 1.0

Erstellt von: Christian Kuss, Darja Amelcenko, Niccolo Langenheim (Luther Rechtsanwaltsgesellschaft mBH) und René Seydel, Dr. Franka Grünewald, Dr. Tanja Röchert-Voigt (DigitalAgentur Brandenburg)

1 Kontext

Digitale Kollaborationswerkzeuge sind ein Grundbestandteil von New Work Arbeitsszenarien. Diese Werkzeuge sind dafür ausgelegt, dass Personen synchron oder asynchron, von verschiedenen Arbeitsplätzen aus gemeinsam an Dokumenten und Medien arbeiten. Dies ist insbesondere für Institutionen- oder Standort-übergreifende Szenarien ein beliebter Weg, schnell Gedanken auszutauschen und Arbeitsschritte voranzubringen, ohne den Arbeitsort wechseln zu müssen.

Der schnelle Austausch mit Kollaborationswerkzeugen wird auch bei Mitarbeitenden der Verwaltung immer beliebter. Solche Werkzeuge müssen – anders als in der privaten Wirtschaft – über Ausschreibungen bzw. Vergabeverfahren beschafft werden. Dabei gilt es, Aspekte des Datenschutzes und der Informationssicherheit frühzeitig zu beachten und auch schon bei der Ausschreibung zu berücksichtigen. Welche wichtigen Aspekte sind aus der Perspektive der Vergabe, des Datenschutzes und der IT-Sicherheit zu beachten?

Dieser Fragestellung hat sich die DigitalAgentur Brandenburg zusammen mit der Kanzlei Luther in einem praxisorientierten Workshop gewidmet, in dem der Prozess von der Idee, eine kollaborative Softwareanwendung einzusetzen, bis zum tatsächlichen Einsatz durchgesprochen wurde.

Als Zusammenfassung und Handlungsleitfaden ist folgende Checkliste entstanden, die bei der Entscheidung für, Ausschreibung von und der Einführung einer kollaborativen Software in der Behörde unterstützen soll.

2 Checkliste

1. Marktsichtung und Definition der Anforderungen

1. Betrachtung der Art der zu verarbeitenden Daten und des Zwecks
   - werden personenbezogene oder personenbeziehbare Daten verarbeitet?
   - Falls ja:?
     - Welche Daten werden bei der Registrierung verarbeitet?
     - Mit welchen Daten wird/kann/darf in der Anwendung umgegangen werden (inhaltliche Daten)
     - Welche Metadaten fallen an?
   - Welchen Schutzbedarf haben die zu verarbeitenden Daten?
   - Achtung: Diese Betrachtung ist eine wichtige Grundlage für die nachfolgenden Schritte. Der Schutzbedarf ist wichtig bei der Risikobetrachtung und den daraus abzuleitenden technischen und organisatorischen Schutzmaßnahmen (TOMs).
2. Ist die Datenverarbeitung rechtmäßig?
   - Zu welchem Zweck werden Daten verarbeitet?
   - Zu welchem Zweck soll kollaborativ zusammengearbeitet werden?
   - Gibt es eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten?
   - Ist die Datenverarbeitung erforderlich für die Zwecke?
   - Gibt es eine sinnvolle und zumutbare Alternative?
3. Betrachtung der IT-Sicherheitstechnischen Aspekte
   - Einbeziehung der für das Anwendungsszenario relevanten IT-Sicherheitsvorgaben und Berücksichtigung der IT-Grundschutz-Bausteine (Orientierung, wenn keine Pflicht).
     - In dem Rahmen kann eine Vorbetrachtung der Anbieter auf dem Markt in Bezug auf die Informationssicherheit stattfinden (Marktrecherche)
     - IT-Sicherheit von Anfang an mitdenken
   - Einbeziehung der in der Institution vorhandenen IT-Sicherheits-Konzeption, Integrationsfähigkeit der Lösung betrachten, ggf. neue Sicherheitskonzeption vordenken
   - Querverbindungen z.B. zum Datenschutz mitdenken

4. Liegt ein Drittlandtransfer der personenbezogenen Daten vor und falls ja, sind die datenschutzrechtlichen Voraussetzungen dafür erfüllt?
    - Gibt es einen Angemessenheitsbeschluss der EU-Kommission?
    - Kommen Standardvertragsklauseln zum Einsatz?
    - Welche zusätzlichen technischen und organisatorischen Maßnahmen gibt es?

5. Wo und wie lange werden die personenbezogenen Daten gespeichert? Wie werden die personenbezogenen Daten gelöscht?
    - Speicherung der Daten innerhalb der EU/EWR
    - Speicherung der Daten bis zur Erreichung des Verarbeitungszwecks
    - Erstellung eines Löschkonzeptes inkl. Löschprozess

6. Prüfung verschiedener Anbieter im Rahmen der Marktsichtung
    - Impressum: Sitz des Anbieters? D, EU oder Drittstaat?
    - Werden die datenschutzrechtlichen Vorgaben eingehalten? (TOMs, Grundsatz der Datenminimierung, Privacy by design/default)
    - Prüfung der Punkte 3 – 5 für jeden Anbieter

2. Ausschreibung und Vergabe

7. Ausschreibung und Vergabe
    - Eignungs- und Zuschlagskriterien müssen getrennt sein
    - Alle Kriterien müssen bei der Vergabe bekannt gemacht werden
    - Tipp: eine Verhandlungsvergabe mit Gespräch kann der Absicherung beider Parteien dienen
    - Der Vertrag ist Teil der Vergabe und entsteht optimalerweise aus der Leistungsbeschreibung
    - Sicherheitskonzeption für Ausschreibung berücksichtigen und gegebenenfalls mit ausschreiben

8. Abschluss eines Auftragsverarbeitungsvertrages
    - Wie sind die Rollen der Beteiligten?

3. Einführung der Software in der Organisation

9. Erstellung einer IT-Sicherheitskonzeption die den Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten Information und den verarbeitenden Systemen entspricht
    - Einbeziehung der in der Institution vorhandenen IT-Sicherheits-Konzeption, ggf. Integration
    - Berücksichtigung der Vorgaben des Landes und der Institution
    - Umsetzung nach der Methodik des BSI-Grundschutzes (Orientierung, wenn keine Pflicht)
10. Implementierung eines Prozesses zur Abhilfe von Betroffenenrechten (mit anderen Verantwortlichen/Auftragsverarbeitern)
11. Erstellung eines Verarbeitungsverzeichnisses
12. Überprüfung, ob eine Datenschutzfolgenabschätzung notwendig ist:
    - Schutzbedarfsfeststellung anhand der Art der Daten
    - Risikoermittlung
13. Aktualisierung der eigenen Datenschutzerklärung, soweit neue IT-Tools eingesetzt werden
14. Erstellung von Handlungsanweisungen bei der Verwendung komplexer IT-Tools & Durchführung von Schulungen der Mitarbeiter:innen

Impressum

Angaben gemäß §5 TMG

DigitalAgentur Brandenburg GmbH
Schiffbauergasse 14
14467 Potsdam

Vorsitzender des Aufsichtsrats:
Staatssekretär Hendrik Fischer

Handelsregister: HRB31591
Registergericht Potsdam

Vertreten durch:
Herrn Dr. André Göbel

Kontakt

Telefon: 0331.660-4000
Telefax: 0331.660-64000
E-Mail: kontakt@digital-agentur.de

Gefördert durch das
Ministerium für Wirtschaft, Arbeit und Energie des Landes Brandenburg

Version 1.0