Checkliste zur Umsetzung von Privacy by Design / Privacy by Default

1. *Prüfung der Rechtsgrundlage der Datenerhebung und Verarbeitung:*
    a. Ist eine Datenerhebung erlaubt?
    b. Auf welcher Rechtsgrundlage?
    c. Ist eine Einwilligung zur Datenerhebung und -verarbeitung notwendig?

2. *Zweckbindung*
    a. Für welchen Zweck werden die personenbezogenen Daten erhoben? (Definition und Beschreibung)
    b. Sollen die Daten für einen anderen als den ursprünglichen Zweck genutzt werden?
    c. Ist für die Zweckänderung eine Einwilligung notwendig?

3. *Datensparsamkeit*
    a. Welche Daten sollen erhoben werden?
    b. Besteht die Möglichkeit einer anonymen oder pseudonymen Erhebung bzw. Nutzung?
    c. Welche zusätzlichen Daten sollen erhoben werden? Welche Voraussetzungen sind dafür notwendig?

4. *Transparenz und Information*
    a. Wie können die Nutzer über die Datenverarbeitung ausreichend informiert werden (z.B. Datenschutzerklärung, AGB bzw. Nutzungsbedingungen)?
    b. Sind die Risiken für die Nutzer benannt und gibt es Hinweise zur Minimierung?
    c. Wo sind opt-out Möglichkeiten zu implementieren (z.B. Widerspruchsmöglichkeit bei Trackingverfahren)?
    d. Wie können die Privatsphäreeinstellungen integriert werden?

5. *Rechte der Betroffenen*
    a. Wie können die Nutzer Auskunft über die gespeicherten Daten erhalten?
    b. Wie können Daten berichtigt werden?
    c. Ist ein Löschkonzept hinterlegt bzw. können Daten gesperrt werden, wenn ein Löschen nicht möglich ist?
    d. Wie können die Nutzer einer eingewilligten Datenverarbeitung widersprechen?
    e. Wie wird die Umsetzung eines Widerspruches sichergestellt?

6. *Informationssicherheit – Umsetzung technische und organisatorische Maßnahmen*
    a. Wie kann die Anwendung technisch abgesichert werden?
    b. Welche Möglichkeiten hat der Nutzer seine Daten zu schützen (z.B. 2-Faktor-Authentisierung)?
    c. Wie müssen die internen Prozesse gestaltet sein, um die IT-Sicherheit zu gewährleisten?
    d. Werden Dienstleister benötigt?
    e. Welche Voraussetzungen müssen die Dienstleister erfüllen?
    f. Wie kann die Sicherheit bei den Dienstleistern gewährleistet und überprüft werden?