Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf

in Anlehnung an die
Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter[1]

[1] Dieser Prüfkatalog bezieht sich auf Apps, die dem TMG unterfallen; die genannte Orientierungshilfe ist abrufbar unter https://www.lda.bayern.de/media/oh_apps.pdf

App-Name: _____

Zweck der App: _____

Hauptfunktion(en): _____

Plattform: _____

Verantwortliche Stelle: _____

App Store (URL): _____

Geprüfte App-Version: _____

Datei-Größe: _____

Packetname: _____

Prüfsumme: _____

Prüfdatum: _____

Prüfer: _____

I. Arten personenbezogener Daten[2]

1. Welche Nutzungsdaten (vgl. § 15 Abs. 1 TMG) werden von der App automatisch verarbeitet?

2. Welche Bestandsdaten (vgl. § 14 Abs. 1 TMG) werden von der App automatisch verarbeitet?

3. Welche Inhaltsdaten werden von der App automatisch verarbeitet?

4. Werden besondere Arten von personenbezogenen Daten (vgl. insb. Art. 15 Abs. 7 BayDSG) eingesetzt?
   ☐ Gesundheitsdaten ☐ Kreditkartendaten ☐ Andere ☐ Nein
   Bemerkung:

[2] Es wird darauf hingewiesen, dass sich die rechtlichen Vorgaben bzgl. der folgenden Hauptabschnitte (I. bis XII.) primär aus dem TMG und dem BayDSG ergeben. Daneben können im Einzelfall aber auch spezialgesetzliche Vorschriften (z.B. § 78a SGB X) Anwendung finden.

II. Datenschutzbestimmungen (die Vorgaben der §§ 13 ABs.1, 5 TMG sind zu beachten)

5. Sind die Datenschutzbestimmungen bereits im App-Store einsehbar
(z. B. über die von Google bereitgestellte Funktion „Datenschutzerklärung für Entwickler")?
☐ Ja ☐ Nein, Begründung:[3]

6. Sind die Datenschutzbestimmungen bei erstmaliger App-Nutzung sofort einsehbar (z. B. Pop-Up oder Info-Frame)?
☐ Ja ☐ Nein, Begründung:

7. Sind die Datenschutzbestimmungen innerhalb der App leicht auffindbar und einsehbar?
☐ Ja ☐ Nein, Begründung:

8. Handelt es sich um Datenschutzbestimmungen speziell für die App (z B. anstelle der Datenschutzerklärung der Webseite)?
☐ Ja ☐ Nein, Begründung:

9. Wird in den Datenschutzbestimmungen die Erhebung, Verarbeitung und Nutzen personenbezogener Daten ausreichend beschrieben?
☐ Ja ☐ Nein, Begründung:

10. Werden in den Datenschutzbestimmungen die Berechtigungen der App inklusive deren Verwendung ausreichend beschrieben?
☐ Ja ☐ Nein, Begründung:

11. Liegt ein den Anforderungen von § 5 TMG („leicht erkennbar", „unmittelbar erreichbar", „ständig verfügbar"; zudem ggf. § 55 Abs. 2 RStV-Anforderung) entsprechendes Impressum vor?
☐ Ja ☐ Nein, Begründung:

[3] Die Fragen sind so gestellt, dass im Allgemeinen ein "Ja" zu erwarten ist. Bei einer Abweichung muss eine Begründung vorgelegt werden, anhand derer zu prüfen ist, ob insoweit von den entsprechenden Vorgaben im Einzelfall ausnahmsweise abgewichen werden kann.

III. Berechtigungen

12. Welche Berechtigungen erhält die App auf dem Gerät?

Name und Art der Berechtigung:	Zugriff auf personenbezogene Daten möglich?
12.1. _____	☐ Ja ☐ Nein
12.2. _____	☐ Ja ☐ Nein
12.3. _____	☐ Ja ☐ Nein
12.4. _____	☐ Ja ☐ Nein
12.5. _____	☐ Ja ☐ Nein
12.6. _____	☐ Ja ☐ Nein
12.7. _____	☐ Ja ☐ Nein
12.8. _____	☐ Ja ☐ Nein
12.9. _____	☐ Ja ☐ Nein

13. Werden nur Berechtigungen eingefordert, die für die Funktion der App zwingend benötigt werden?
☐ Ja ☐ Nein, Begründung:

14. Wird eine (ausreichende) Einwilligung des Nutzers zuvor abgefragt (beachte § 13 Abs. 2, 3 TMG)?
☐ Ja ☐ Nein, Begründung:

IV. Zugangsdaten (Vorgaben des § 13 Abs. 4 TMG bzw. Art. 7 BayDSG sind zu beachten)

15. Besteht die Möglichkeit einer Registrierung und Anmeldung in der App mit eigenen Zugangsdaten (Benutzername und Passwort)?

☐ Ja ☐ Nein

Falls ja, welche Daten werden für die Registrierung und Anmeldung genutzt:

Falls 15. „Ja", weitere Fragestellungen:

15.1. Werden ausreichend komplexe Passwörter (mind. 8-stellig mit Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen) erzwungen/durch Darstellung empfohlen?

☐ Ja ☐ Nein, Begründung:

15.2. Werden keine anderen gerätebezogenen Daten (z.B. IMEI-Nummer) als Identifizierungswert im Rahmen der Authentifizierung verwendet?

☐ Werden nicht verwendet ☐ Werden verwendet, weil:

15.3. Werden die Zugangsdaten des Nutzers lokal gespeichert?

☐ Ja ☐ Nein

15.3.1. Werden die Zugangsdaten im geschützten App-Bereich gespeichert?

☐ Ja ☐ Nein ☐ Nicht anwendbar

Bemerkung:

15.3.2. Werden die Zugangsdaten mit einem für die Passwortspeicherung geeignetem kryptographisches Verfahren (z. B. KeyChain bei iOS, PBKDF2 bei Eigenimplementierung) transformiert, bevor diese lokal gespeichert werden?

☐ Ja ☐ Nein ☐ Nicht anwendbar

Bemerkung:

15.4. Werden die Zugangsdaten des Nutzers auf einem Server gespeichert?

☐ Ja ☐ Nein

Bemerkung:

15.4.1. Werden die Zugangsdaten kryptographisch verarbeitet (d. h. nicht im Klartext) lokal gespeichert?

☐ Ja ☐ Nein ☐ Nicht anwendbar

Bemerkung:

15.4.2. Wird ein für die Passwortspeicherung geeignetes kryptographisches Verfahren (z. B. PBKDF2 bei Eigenimplementierung) eingesetzt, um die Zugangsdaten zu speichern?

☐ Ja ☐ Nein ☐ Nicht anwendbar

Bemerkung:

15.5. Werden in der App lokale Session-Timeouts in Abhängigkeit des jeweiligen Schutzbedarfs eingesetzt, die ein erneutes Einloggen nach einer gewissen inaktiven Zeit erzwingen?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

15.6. Werden Passwörter bei der Eingabe in der App maskiert (evtl. auswählbar) um ein „Shoulder-Surfing" zu verhindern?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

15.7. Werden Passwörter bei einer „Passwort vergessen"-Funktion über einen zeitlich begrenzen Weblink zurückgesetzt?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

V. Datenübertragungen (insbesondere die Vorgaben des § 13 Abs. 4 TMG bzw. Art. 7 BayDSG sowie Art. 6, 18, 19, 21 BayDSG sind zu beachten)

16. An welche Server werden Daten abgehend vom Gerät übertragen?

	IP-Adresse/Domainname:	Unternehmen/ Behörde:	Innerhalb des EWR?		Rechtsgrundlage geregelt?	
16.1.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein
16.2.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein
16.3.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein
16.4.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein
16.5.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein
16.6.	_____	_____	☐ Ja	☐ Nein	☐ Ja	☐ Nein

Bemerkung/Begründung:

17. Welche Daten werden dabei an welchen Empfänger zu welchem Zweck übertragen?

Daten:	Verantwortliche Stelle:	personen-bezogen?		Zweck:
_____	_____	☐ Ja	☐ Nein	_____
_____	_____	☐ Ja	☐ Nein	_____
_____	_____	☐ Ja	☐ Nein	_____
_____	_____	☐ Ja	☐ Nein	_____
_____	_____	☐ Ja	☐ Nein	_____

_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____
_____	_____	□ Ja	□ Nein	_____

18. Erfolgt eine verschlüsselte Datenübertragung (mit HTTPS)?

□ Ja □ Nein, Begründung: □ Nicht anwendbar

Bemerkung/Begründung:

19. Wird Perfect Forward Secrecy bei HTTPS eingesetzt?

□ Ja □ Nein, Begründung:

Bemerkung/Begründung:

20. Wird TLS1.2 bei HTTPS eingesetzt?

□ Ja □ Nein, Begründung:

Bemerkung/Begründung:

21. Ist SSLv2 und SSLv3 bei HTTPS deaktiviert?
    ☐ Ja ☐ Nein, Begründung:
    Bemerkung/Begründung:

22. Ist die Schlüssellänge bei asymmetrischen Verfahren ausreichend lang (4096-Bit bei RSA, 256-Bit bei EC)?
    ☐ Ja ☐ Nein, Begründung:
    Bemerkung/Begründung:

23. Wird verhindert, dass personenbezogene Daten über HTTP-GET-Parameter übertragen werden?
    ☐ Ja ☐ Nein, Begründung: ☐ Nicht anwendbar
    Bemerkung/Begründung:

24. Werden vertrauenswürdige SSL-Zertifikate verwendet und diese auch zur Verhinderung von Man-In-The-Middle Angriffen überprüft?
    ☐ Ja, welche: ☐ Nein, Begründung: ☐ Nicht anwendbar
    Bemerkung/Begründung:

25. Wird SSL-Pinning (feste „Verdrahtung" des SSL-Zertifikats in der App) eingesetzt?
    ☐ Ja: ☐ Nein, Begründung: ☐ Nicht anwendbar
    Bemerkung/Begründung:

26. Werden Token-Werte statt Account-Daten (z. B. Kundennummer) für einen Session-Bezug zum Backend verwendet?
    ☐ Ja ☐ Nein, Begründung: ☐ Nicht anwendbar
    Bemerkung/Begründung:

VI. Speicherung von App-Daten

27. Welche Daten werden lokal auf dem Gerät gespeichert?

Daten:	Personenbezogen?
_____	☐ Ja ☐ Nein
_____	☐ Ja ☐ Nein
_____	☐ Ja ☐ Nein
_____	☐ Ja ☐ Nein
_____	☐ Ja ☐ Nein

28. Werden personenbezogenen Daten nur gespeichert, soweit und solange sie für den Betrieb der App notwendig sind?

☐ Ja ☐ Nein (wieso) ☐ Nicht anwendbar

Bemerkung/Begründung:

29. Werden Daten auf der externen SD-Karte des Geräts gespeichert (falls anwendbar)?

☐ Ja (welche und wieso) ☐ Nein ☐ Nicht anwendbar

Bemerkung/Begründung:

30. Werden die (auf der SD-Karte) gespeicherten Daten nach Deinstallation der App gelöscht (falls anwendbar)?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

31. Werden Inhalts- oder Nutzungsdaten der App durch einen Cloud-Backup-Mechanismus des Endgeräts gespeichert, sofern dieser grundsätzlich vom Nutzer aktiviert ist?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

VII. Backend

32. Ist das Backend gegen Angriffe auf Basis von OWASP-Top 10 (2013) ausreichend geschützt?

    ☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

    Bemerkung/Begründung:

33. Kann der Backend-Webserver statt über HTTPS auch über HTTP aufgerufen werden (z. B. SSL-Stripping-Angriff)?

    ☐ Ja (wieso) ☐ Nein ☐ Nicht anwendbar

    Bemerkung/Begründung:

VIII. Logging

34. Welche Logging-Varianten in der App werden in der Produktivversion eingesetzt?

    ☐ System-Log ☐ Remote-Log ☐ File-Log ☐ Keine ☐ Andere ☐ Nicht anwendbar

    Bemerkung:

35. Werden personenbezogene Daten geloggt?

    ☐ Ja ☐ Nein ☐ Nicht anwendbar

    Bemerkung:

IX. Tracking (z.B. Reichweitenmessung)

(soweit einschlägig - § 15 Abs. 3 TMG ist zu beachten)

36. Werden Trackingverfahren in der App eingesetzt?

☐ Ja (welche) ☐ Nein

Bemerkung/Begründung:

Falls „Ja", weitere Fragestellungen:

36.1. Wird die IP-Adresse vor der systematischen Verarbeitung (z.B. Geolokalisierung) ausreichend anonymisiert?

☐ Ja: ☐ Nein (wieso nicht)

Bemerkung/Begründung:

36.2. Wird in den Datenschutzbestimmungen ausreichend darüber informiert?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

36.3. Existiert für den Nutzer eine jederzeit leicht auffindbare Widerspruchsmöglichkeit (z.B. durch eine Opt-Out-Möglichkeit) innerhalb der App?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

36.4. Existiert ein Vertrag zur Auftragsdatenverarbeitung mit dem Dienstleister (falls Reichweitenmessung nicht selbst betrieben)?

☐ Ja ☐ Nein (weiso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

36.5. Werden eindeutige (Geräte-) IDs vergeben/verwendet?

☐ IMEI ☐ IMSI ☐ MAC-Adresse ☐ Unique-IDs ☐ Andere:

Bemerkung:

36.6. Welche Tracking-Cookies werden eingesetzt?

Cookie-Name:	Zweck:
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

X. In-App-Browser-Engine (z.B. Webkit)

37. Wird ein In-App Browser eingesetzt?

☐ Ja ☐ Nein ☐ Nicht anwendbar

Bemerkung:

Falls „Ja", weitere Fragestellungen:

38. Ist ein (JSON-)SSLStrip-Angriff möglich?

☐ Ja (wieso) ☐ Nein ☐ Nicht anwendbar

Bemerkung/Begründung:

39. Wird der HTTP „no-store“ Header vom Backend zur Verhinderung der Speicherung von Cachedaten gesendet?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

40. Ist ein Whitelist-Schema für URLs implementiert?

☐ Ja ☐ Nein (wieso) ☐ Nicht anwendbar

Bemerkung/Begründung:

41. Ist ein Caching von Webformulardaten deaktiviert?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

42. Ist Javascript disabled (deaktiviert), falls es nicht benötigt wird?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

43. Sind Plugins disabled (deaktiviert), falls sie nicht notwendig sind?

☐ Ja ☐ Nein (wieso nicht) ☐ Nicht anwendbar

Bemerkung/Begründung:

XI. Geolokalisierung

44. Wird in der App auf Standortdaten des Geräts zugegriffen?

☐ Ja ☐ Nein

Bemerkung:

Falls „Ja", weitere Fragestellungen:

44.1. Werden Standortdaten nur in der unbedingt nötigen Auflösung („Verwaschung") erfasst?

☐ Ja ☐ Nein (wieso nicht)

Bemerkung/Begründung:

44.2. Werden genaue Standortdaten nur lokal verarbeitet („Rasterbereich")?

☐ Ja ☐ Nein (wieso nicht)

Bemerkung/Begründung:

44.3. Werden Standortdaten lokal gespeichert?

☐ Ja (wieso) ☐ Nein

Bemerkung/Begründung:

44.4. Werden Standortdaten an das Backend übertragen?

☐ Ja (wieso erfolgt keine lokale Standortverarbeitung) ☐ Nein

Bemerkung/Begründung:

44.5. Sind die Abtastintervall der Standortdaten so groß wie möglich?

☐ Ja ☐ Nein, Begründung:

44.6. Besteht die Möglichkeit, die Lokalisierung auszuschalten

☐ Ja ☐ Nein, Begründung:

XII. Inhaltsdaten

45. Werden in Bezug auf die Verarbeitung von personenbezogenen Inhaltsdaten die jeweiligen (ggf. besonderen) datenschutzrechtlichen Anforderungen nach dem jeweils einschlägigen Fachrecht beachtet?

    □ Ja □ Nicht anwendbar

    Bemerkung:

Anhang: Kurzcheckliste TLS

1. Ausschließlich TLS1.2 (Kein SSL3, TLS1.0, TLS1.1 mehr)
2. Ausschließlich Cipher-Suites, die Perfect Forward Secrecy unterstützen
3. SSL-Pinning (Empfohlen ist Public-Key-Pinning, ausnahmsweise auch CA-Pinning)
4. Auswahl einer vertrauenswürdigen Cerificate-Authority
5. Zertifikate mit 4096-Bit RSA
6. Kein SHA-1 bei der Signierung von Zertifikaten (Statt dessen mind. SHA-256)
7. Keine veralteten kryptographischen Algorithmen (z.B. RC4, DES, ...)
8. Keine Unterstützung von http auf demselben Server (Gefahr von SSL-Stripping-Angriffen)
9. Aktuelles und systematisches Patch-Management (z.B. wegen Heartbleed, Poodle, CCS-Attacken,...) der SSL-Komponenten
10. TLS-Client-Zertifikate zur Erschwerung von Man-in-the-Middle-Attacken