dsb

datenschutzbeauftragte
kanton zürich

Leitfaden

Entwicklung datenschutzkonformer Apps

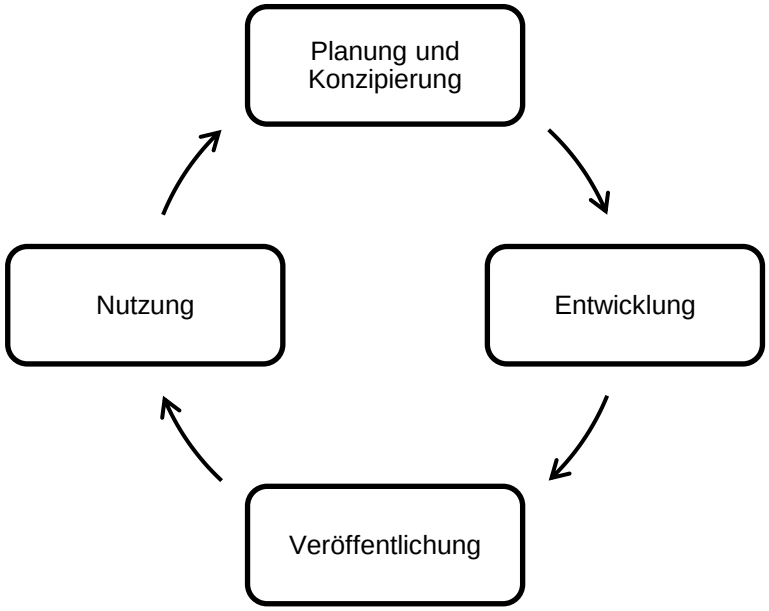
Inhalt

1 Einleitung

Die Verbreitung von mobilen Geräten wie Smartphones oder Tablet-Computer haben den mobilen Apps (Anwendungssoftware für Mobilgeräte) zu einem Boom verholfen. Über die App-Stores lassen sich die mobilen Apps direkt und unkompliziert auf dem Gerät installieren und nutzen. Auch öffentliche Organe stellen Apps zur Verfügung, die staatliche Dienstleistungen anbieten und eine direkte Kommunikation zwischen dem Organ und der Bevölkerung ermöglichen.

Dieser Leitfaden ermöglicht öffentlichen Organen, die App datenschutzkonform zu gestalten. Er richtet sich an Entscheidungsträger und -trägerinnen, Projektleitende und involvierte Personen, die eine App entwickeln oder entwickeln lassen. Im Fokus liegen dabei Apps, die von Bürgerinnen und Bürgern für Transaktionen mit den öffentlichen Organen verwendet werden.

Der Lebenszyklus einer App lässt sich in die vier Phasen Konzipierung, Entwicklung, Veröffentlichung und Nutzung einteilen. In jeder Phase sind unterschiedliche Gesichtspunkte in Bezug auf den Datenschutz und die Informationssicherheit zu beachten. Der Leitfaden ist gemäss dem Lebenszyklus gegliedert.



2 Planung und Konzipierung

Das Bearbeiten von Personendaten durch öffentliche Organe des Kantons Zürich unterliegt dem Gesetz über die Information und den Datenschutz (IDG, LS 170.4). Bearbeitet ein öffentliches Organ mit einer App Personendaten, sind die datenschutzrechtlichen Grundsätze einzuhalten. Dies bedeutet, dass:

- die Gesetzmässigkeit eingehalten werden muss (§ 8 Abs. 1 und Abs. 2 IDG)
- das Verhältnismässigkeitsprinzip beachtet werden muss (§ 8 Abs. 1 IDG)
- die Personendaten nur zweckgebunden bearbeitet werden dürfen (§ 9 IDG)
- die Beschaffung der Personendaten erkennbar sein muss (§ 12 IDG)
- die organisatorischen und technischen Massnahmen zur Gewährleistung der in § 7 IDG verankerten Schutzziele implementiert werden müssen

Bei der Planung und Konzipierung einer App sind die folgenden 7 Schritte zu beachten:

- ➔ **Schritt 1:** Prüfen, ob und welche Personendaten bearbeitet werden.
- ➔ **Schritt 2:** Abklären, ob und welche Rechtsgrundlage für die Datenbearbeitung besteht.
- ➔ **Schritt 3:** Sicherstellen, dass nur die notwendigen Personendaten bearbeitet werden.
- ➔ **Schritt 4:** Klären, zu welchem Zweck die Personendaten in der App bearbeitet werden.
- ➔ **Schritt 5:** Datenschutzerklärung und Nutzungsbedingungen verfassen.
- ➔ **Schritt 6:** Prüfen, ob die App der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen ist.
- ➔ **Schritt 7:** Konsequente Umsetzung von Privacy by Default und Privacy by Design

2.1 Prüfen, ob und welche Personendaten bearbeitet werden

Die folgenden Informationen werden beim Einsatz einer App oft bearbeitet. Sie können Rückschlüsse auf eine natürliche Person gewähren und sind deshalb Personendaten (§ 3 Abs. 3 IDG):

- IP-Adresse oder Mobilnummer (MSISDN)
- Geräte- und Kartenkennung (IMEI, UDID, IMSI, MAC-Adresse)
- Name des mobilen Geräts
- Standort- und Nutzungsdaten
- Fotos, Videos und Audiodateien
- Biometrische Daten (z.B. Fingerabdruck, Gesichtserkennung)
- Kontaktdaten und Kalendereinträge
- Registrierungs- und Kontoverbindungsdaten
- Anruflisten und Nachrichten

Bei der Planung einer App muss das öffentliche Organ prüfen, welche Personendaten einerseits im Zusammenhang mit den erbrachten Dienstleistungen bearbeitet werden, andererseits welche weiteren personenbezogenen Informationen durch den Betrieb der App und die Einräumung von Rechten bearbeitet werden. Diese Datenbearbeitungen sind hinsichtlich Gesetzmässigkeit (Ziffer 2.2) und Verhältnismässigkeit (Ziffer 2.3) zu prüfen.

Durch die Bearbeitung zahlreicher Personendaten kann ein Persönlichkeitsprofil entstehen. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt. Persönlichkeitsprofile sind besondere Personendaten, für deren Bearbeitung höhere Anforderungen zu erfüllen sind. Das öffentliche Organ muss sich insbesondere auf eine hinreichend bestimmte Regelung in einem formellen Gesetz stützen können (§ 8 Abs. 2 IDG).

2.2 Prüfen, ob und welche Rechtsgrundlage für die Datenbearbeitung besteht

Die Rechtsgrundlage für eine Datenbearbeitung in einer App (§ 8 Abs. 1 IDG) kann sich direkt aus einer Norm ergeben oder indirekt aus der Umschreibung einer Aufgabe in einer Norm. Die Datenbearbeitung in einer App muss nicht ausdrücklich in der Rechtsgrundlage erwähnt sein, sie muss aber in einem sachlichen Zusammenhang mit einer durch das öffentliche Organ zu erfüllenden Aufgabe stehen.

2.3 Sicherstellen, dass nur die notwendigen Personendaten bearbeitet werden

Die Datenbearbeitung durch ein öffentliches Organ muss für dessen Aufgabenerfüllung geeignet und erforderlich sein (Verhältnismässigkeit, § 8 Abs. 1 IDG). Die Personendaten müssen dem öffentlichen Organ einerseits die Aufgabenerfüllung ermöglichen (Geeignetheit). Andererseits muss das öffentliche Organ ohne die Personendaten seine Aufgabe nicht erfüllen können (Erforderlichkeit).

Das Prinzip der Verhältnismässigkeit ist im technischen Bereich durch Massnahmen der Datenvermeidung und der Datensparsamkeit umzusetzen. Der Zugriff der App auf andere Anwendungen eines mobilen Geräts ist auf das Notwendige zu beschränken. Damit dürfen nur diejenigen Personendaten erhoben werden, die für das Funktionieren der App erforderlich sind (Grundsatz der Datensparsamkeit, § 11 IDG). Es darf keine Datenbeschaffung auf Vorrat stattfinden.

2.4 Prüfen, zu welchem Zweck die Personendaten bearbeitet werden

Personendaten, die zu einem Zweck erlangt wurden, dürfen nur mit Einwilligung der betroffenen Person oder gestützt auf eine rechtliche Bestimmung für einen anderen Zweck oder eine andere Aufgabe verwendet werden (§ 9 Abs. 1 IDG). Werden beim Tätigen eines Notrufs beispielsweise Ortungsdaten erfasst, dürfen diese nicht bei der in der App ebenso angebotenen Recherchemöglichkeit zu Meldungen des öffentlichen Organs ausgewertet werden.

Für jede Aufgabe des öffentlichen Organs, die mit einer App erfüllt wird, ist separat zu prüfen, ob eine Rechtsgrundlage für die Datenbearbeitung besteht und die Datenbearbeitung verhältnismässig erfolgt.

2.5 Datenschutzerklärung und Nutzungsbedingungen verfassen

Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein (§ 12 Abs. 1 IDG). Diese Transparenz kann mit einer Datenschutzerklärung und Nutzungsbedingungen gewährleistet werden (siehe Ziffer 4).

2.6 Prüfen, ob die App der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen ist

Öffentliche Organe müssen der Datenschutzbeauftragten Projekte und Vorhaben zur Vorabkontrolle unterbreiten, wenn diese Datenbearbeitungen beinhalten, die für die betroffenen Personen mit besonderen Risiken für ihre Rechte und Freiheiten verbunden sind (§ 10 IDG i.V.m. § 24 IDV). Solche Risiken können beispielsweise sein:

- die Sammlung einer Vielzahl besonderer Personendaten
- der Einsatz neuer Technologien
- die gemeinsame Bearbeitung von Personendaten durch mindestens drei verschiedene öffentliche Organe
- eine grosse Anzahl von betroffenen Personen

Das Merkblatt Vorabkontrolle umschreibt, wie bei einer Vorabkontrolle vorzugehen ist.

2.7 Konsequente Umsetzung von Privacy by Design und Privacy by Default

Mit Privacy by Default respektive Privacy by Design wird der Datenschutz und die Informationssicherheit während des ganzen Prozesses gewährleistet. Dafür müssen diese Prinzipien Teil des Konzepts, der Architektur und auch bei einer Vergabe oder Ausschreibung konsequent eingefordert werden.

Ein Beispiel einer Umsetzung: Bei einer App für die Meldung von defekten Strassenlampen müssen die Anwenderin oder der Anwender die Standortdienste selber aktivieren.

3 Entwicklung

3.1 Informationssicherheit während dem Entwicklungsprozess

Bei der Entwicklung einer App jeden Typs (Native-, Web- oder Hybride-Apps) sind die folgenden Punkte zu beachten:

- Erhebung der Gefährdung und der benötigten Massnahmen durch eine Risikoanalyse z.B. Threat modeling[1]
- Anwendung eines Entwicklungsprozesses, der die Informationssicherheit unterstützt, wie z.B. der Secure Development Life Cycle[2]
- Verwendung eines Software Development Kits (SDK) und eines entsprechenden Frameworks für die Softwareentwicklung
- Einsatz und Verwendung von Standard-Software-Bibliotheken, aktuellen Verschlüsselungsalgorithmen und Betriebssystemfunktionen
- Verwaltung des Source Codes in einem zentralen Repository, das die Nachvollziehbarkeit des Codes gewährleistet
- Regelmässiger Code-Review und Anwendung des Vier-Augen-Prinzips bei der Freigabe von kritischen Programmteilen
- Security Audit und Penetration Test der App und der verwendeten Infrastruktur
- Modularer Aufbau der App
- Einsatz eines App-Hardening-Programms, vor allem für den Laufzeitschutz

Sofern die App mit einer zentralen Webapplikation kommuniziert, bestehen zusätzliche Anforderungen für die datenschutzkonforme und sichere Gestaltung der Webapplikation. Siehe Merkblatt Anforderungen an eine sichere Website.

3.2 Verantwortlichkeit beim Outsourcing

Das öffentliche Organ ist für die Datenbearbeitungen durch die App verantwortlich, auch wenn diese an einen Dritten übertragen werden (Auftragsdatenbearbeitung, Outsourcing), beispielsweise wenn der Betrieb der App an einen Anbieter entsprechender Dienstleistungen ausgelagert wird.

Die Inanspruchnahme von Dienstleistungen zur Entwicklung der App-Software oder Erstellung von Masken und Illustrationen, ohne dass die Beteiligten auf Personendaten, Accounts oder Schnittstellen zugreifen können, ist keine Auslagerung im datenschutzrechtlichen Sinne.

Weitere Informationen sind im Leitfaden Bearbeiten im Auftrag zu finden.

---

[1] Threat Modelling:
- SDL Threat Modeling Tool – Microsoft Corporation
- Application Threat Modeling - Open Web Application Security Project (OWASP)
- Threat model – Wikipedia

[2] Security Development Lifecycle – Mehr Sicherheit durch sichere Entwicklung – scip AG

4 Veröffentlichung

Mit einer Datenschutzerklärung und Nutzungsbedingungen ist Transparenz über die Datenbearbeitung zu schaffen, noch bevor die App heruntergeladen wird. Nach der Installation beim erstmaligen Starten müssen die Nutzerinnen und Nutzer die Nutzungsbedingungen und die Datenschutzerklärung vorgelegt erhalten und diesen aktiv zustimmen (Akzeptieren-Button). Sie müssen so verfasst und dargestellt sein, dass die Nutzerinnen und Nutzer sie tatsächlich lesen und verstehen.

Die Datenschutzerklärung muss Angaben zu folgenden Punkten enthalten (siehe auch Checkliste unter Ziffer 8):

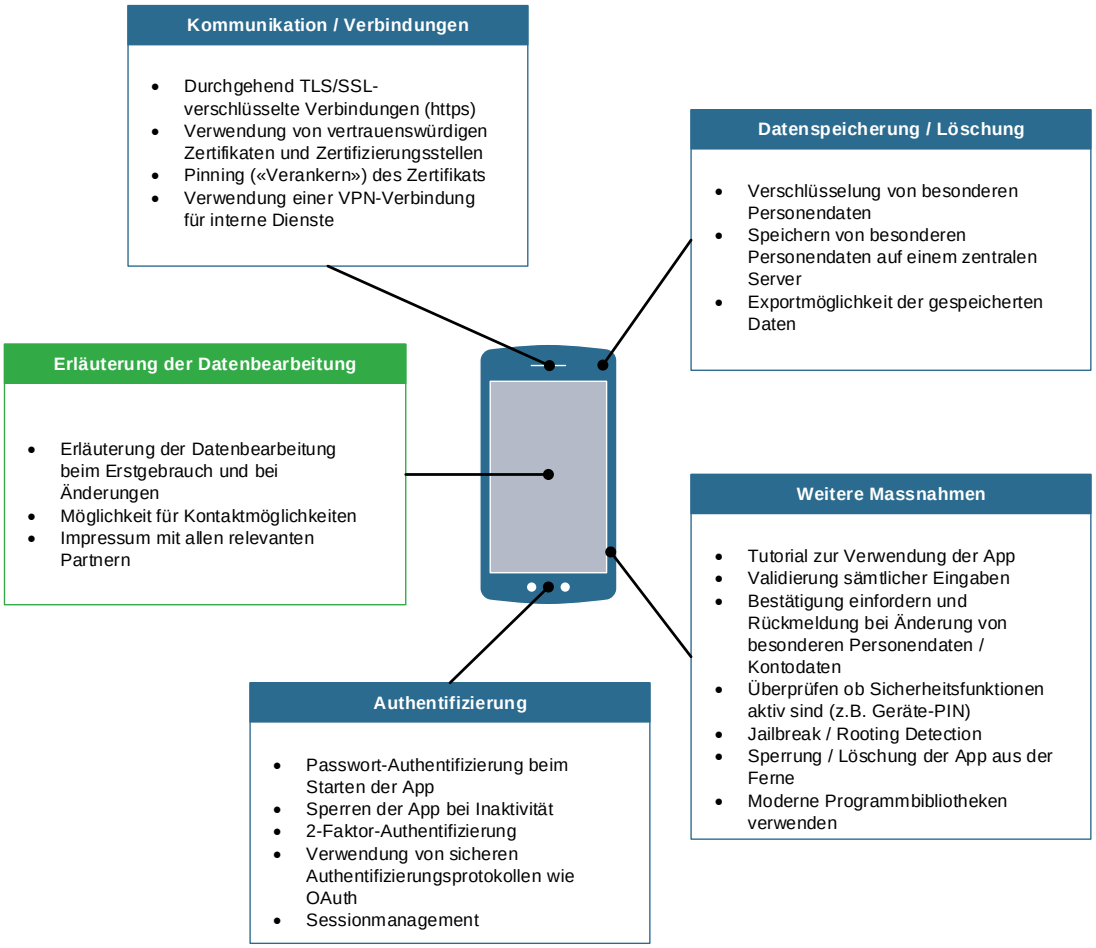
- Verantwortlicher Datenbearbeiter (öffentliches Organ: Kontaktdaten)
- Bearbeitete Personendaten
- Rechtsgrundlage für die Bearbeitung der Personendaten
- Zweck der Bearbeitung der Personendaten (detaillierte Zusammenstellung)
- Erteilte Zugriffsberechtigungen bei Herunterladen oder Zustimmung zu den Nutzungsbedingungen
- Organisatorisch-technische Massnahmen zur Gewährleistung der Schutzziele
- Einbezug von Dritten im Sinne eines Outsourcings
- Eventuelle Bekanntgabe von Personendaten an Dritte (Datenbekanntgabe)
- Aufbewahrungsdauer und Löschungsmechanismen für die Personendaten
- Zuständige Stelle und Ansprechperson für die Rechte der Nutzerinnen und Nutzer (Auskunftsrecht, Berichtigung und Löschung von Personendaten)
- Speicherort der Personendaten (Serverstandort)

Änderungen der Nutzungsbedingungen und Datenschutzerklärung müssen transparent erfolgen. Wenn eine Änderung der Datenbearbeitung beabsichtigt wird, beispielsweise als Folge einer Weiterentwicklung der App oder in Folge einer Änderung der Nutzungsbedingungen, müssen die Nutzerinnen und Nutzer darüber informiert werden und die Möglichkeit erhalten, erneut zuzustimmen. Öffentliche Organe dürfen sich kein jederzeitiges Änderungsrecht ausbedingen.

5 Nutzung

Im Hinblick auf die Nutzung der App sind verschiedene Punkte zur Sicherheit zu beachten und entsprechende Schutzmassnahmen vorzusehen. Vorausgesetzt wird eine sichere Konfiguration des mobilen Gerätes selber (anwenderseitige Massnahmen).

Die nachfolgende Grafik gibt eine Übersicht der wichtigsten organisatorischen Massnahmen sowie der technischen Massnahmen.



5.1 Schutzmassnahmen

Je nach Art, Verwendungszweck und Beschaffenheit ist die App mit unterschiedlichen Schutzmassnahmen zu versehen. Die Akzeptanz kann erhöht werden, wenn die Nutzerinnen und Nutzer die Schutzmassnahmen anpassen können. Den Nutzerinnen und Nutzern müssen dabei Erklärungen gegeben werden, damit diese die Auswirkungen einer Anpassung der Schutzmassnahmen abschätzen können.

Die nachfolgende Tabelle teilt die gängigsten Schutzmassnahmen den Anforderungen bei Personendaten und besonderen Personendaten zu. Fehlt eine Zuteilung, ist die Umsetzung optional, jedoch meistens dennoch sinnvoll.

Schutzmassnahme	**Personendaten**	**Besondere Personendaten**
Authentifizierung		

Schutzmassnahme	**Personendaten**	**Besondere Personendaten**
Starten / Entsperren der App mit einem **PIN / Passwort**	x	x
Bereitstellen einer **Zwei-Faktor-Authentifizierung** für das Starten und Entsperren der App (beispielsweise Fingerabdruck oder Gesichtserkennung)		x
Einsatz eines **Nutzer- (Client-) Zertifikats** für die Zwei-Faktor-Authentifizierung an der zentralen Webapplikation		x
Anwendung von **Standardprotokollen für die Authentifizierung** (z.B. OAuth[3]) an der zentralen Webapplikation		
Sperren der App bei **Inaktivität**		x
Implementierung eines funktionierenden **Sessionmanagements** (Erneuerung des Authentifizierungstoken, Neuanmeldung bei Passwortwechsel usw.)	x	x
Datenspeicherung / Löschung		
Verschlüsselung der Daten, die in der App gespeichert sind		x
Löschen von temporären Daten beim Schliessen der App (z.B. Löschen von zwischengespeicherten Anmeldedaten)	x	x
Datenlöschung bei falschem PIN / Passwort nach einer bestimmten Anzahl Fehlversuchen		x
Abspeichern von besonderen Personendaten **auf einem zentralen Server**		x
Sichere Exportmöglichkeit, um die in der App enthaltenen Daten zu sichern (z.B. für die Migration auf ein neues Smartphone)	x	x
Kommunikation / Verbindungen		
Absichern sämtlicher Kommunikationsverbindungen mit **TLS/SSL-Verschlüsselung** (https)	x	x
Vertrauenswürdige Zertifikate und **Zertifizierungsstellen** (Certificate Authorities) des Betriebssystems verwenden	x	x
Pinning («Verankern») des **Zertifikats** innerhalb der App		x

[3] OAuth: OAuth - Wikipedia

Weitere Massnahmen		
Anbieten eines **Tutorials** für die Nutzung der App (Einführung inkl. Sicherheitsfunktionen)		x
Sämtliche Eingaben der Nutzerinnen oder Nutzer sind client- und serverseitig zu **validieren**	x	x
Änderungen von besonderen Personendaten / Kontodaten durch die Nutzerin / den Nutzer **bestätigen lassen** (zum Beispiel durch Passworteingabe) und Verschicken einer **Info-E-Mail**	x	x
Überprüfen, ob die **Sicherheitsfunktionen** des mobilen Geräts **aktiv** sind, und die Nutzerin / den Nutzer entsprechend informieren (z.B. Geräte-PIN)	x	x
Hinweis an die Nutzerin / den Nutzer bei Erkennung einer Veränderung des Betriebssystems (**Jailbreak / Rooting Detection**[4])	x	x
Möglichkeit der **Datenlöschung oder der Sperrung aus der Ferne**		x
Insbesondere bei Android[5] prüfen, ob **aktuelle Bibliotheken** für **Sicherheitsfunktionen eines Drittherstellers** verwendet werden sollen (z.B. Verschlüsselung)	x	x
Implementierung von weiteren Schutzmassnahmen, wie die Verhinderung von Bildschirmaufnahmen (Screenshots) usw.		x
Die **App an das mobile Gerät binden**, damit sie nicht auf ein anderes Gerät kopiert werden kann		x

5.2 Aufbewahrung der Personendaten

Werden Daten nicht nur lokal in der App, sondern auch zentral beim öffentlichen Organ gespeichert, gelten die üblichen Bestimmungen zur Aufbewahrung von Personendaten.

Für Personendaten, die in einer App bearbeitet und zentral gespeichert werden, gelten die im jeweiligen Bereich anwendbaren Vorschriften zur Aufbewahrungsdauer. Für die Löschung der Daten nach Ablauf dieser Fristen ist ein Mechanismus vorzusehen.

Der Speicherort (Serverstandort) der zentral aufbewahrten Personendaten hat sich nach dem Leitfaden Bearbeiten im Auftrag zu richten. Die Datenschutzerklärung muss die Nutzerinnen und Nutzer über den Speicherort der Personendaten informieren.

[4] Jailbreak / Rooting Detection: Erkennt, ob das vom Hersteller installierte Betriebssystem eines mobilen Geräts verändert wurde.
[5] Die Android-Plattform kann durch den Hersteller selber angepasst werden. Dadurch sind viele unterschiedliche mobile Betriebssysteme mit zum Teil veralteten Versionen im Einsatz.

5.3 Datenschutzrechtliche Ansprüche der Nutzerinnen und Nutzer

Der App-Anbieter muss auf Verlangen der Nutzerin oder dem Nutzer Auskunft über die zu ihrer oder seiner Person bearbeiteten Personendaten geben (§ 20 Abs. 2 IDG). Weiter kann die von einer Datenbearbeitung betroffene Person vom öffentlichen Organ verlangen, dass es unrichtige Personendaten berichtigt oder vernichtet (§ 21 lit. a IDG). Nach Ablauf der Aufbewahrungsdauer besteht der Anspruch auf Löschung der bearbeiteten Personendaten.

5.4 Deinstallation der App

Die Deinstallation der App soll einfach möglich sein. Dabei ist der Export der mit der App gespeicherten Personendaten zu ermöglichen (Datenportabilität). Die nicht mehr benötigten Daten sind zu löschen.

6 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich

- Checkliste Smartphone-Sicherheit
- Leitfaden Bearbeiten im Auftrag
- Merkblatt Anforderungen an eine sichere Website
- Merkblatt Dienste Dritter auf Websites
- Merkblatt Vorabkontrolle

Kanton Zürich, Amt für Informatik

- AGB Auslagerung Informatikleistungen

Kanton Zürich, Staatskanzlei

- Leitfaden für die Entwicklung von Mobile-Apps

Links zu weiteren Informationen

- Mobile Security Project, Open Web Application Security Project (OWASP)
- Baustein CON.8 Software-Entwicklung, Bundesamts für Sicherheit in der Informationstechnik (BSI)
- Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Düsseldorfer Kreis
- Smartphone Secure Development Guidelines for App Developers, European Network and Information Security Agency (ENISA)
- Verbraucherfreundliche Best-Practice bei Apps: Eine Orientierungshilfe für die Praxis, Bundesministerium der Justiz und für Verbraucherschutz

7 Anhang A – Checkliste Entwicklung

Nr.	Checklisten Punkt	Erledigt
Planung und Konzipierung		
1	Prüfen, ob und welche Personendaten bearbeitet werden	☐
2	Abklären, ob und welche Rechtsgrundlage für die Datenbearbeitung besteht	☐
3	Sicherstellen, dass nur die notwendigen Personendaten bearbeitet werden	☐
4	Klären, zu welchem Zweck die Personendaten in der App bearbeitet werden	☐
5	Datenschutzerklärung und Nutzungsbedingungen verfassen	☐
6	Prüfen, ob die App der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen ist	☐
7	Konsequente Umsetzung von Privacy by Default / Privacy by Design	☐
Entwicklung		
8	Gefährdung mit einer Risikoanalyse erhoben und die benötigten Massnahmen umgesetzt	☐
9	Einsatz und Verwendung von Standard-Software-Bibliotheken und Betriebssystemfunktionen sichergestellt	☐
10	Security Audit und Penetration Test der App und der verwendeten Infrastruktur durchgeführt	☐
11	Anforderungen an die Datenbearbeitung im Auftrag bei einem Outsourcing erfüllt	☐
Veröffentlichung		
11	Datenschutzerklärung und Nutzungsbedingungen aktuell und im App-Store publiziert	☐
Sicherheitsmassnahmen bei der Nutzung		
12	Nötige Schutzmassnahmen, gemäss Risikoanalyse umgesetzt, insbesondere für die folgenden Punkte: ■ Authentifizierung ■ Datenspeicherung / Löschung ■ Kommunikation / Verbindung ■ Weitere Massnahmen	☐

8 Anhang B – Checkliste für Datenschutzerklärung, Nutzungsbedingungen, Impressum und Begründung der Berechtigungen

In den Nutzungsbedingungen und der Datenschutzerklärung sind folgende Punkte festzuhalten:

Nr.	Checklisten Punkt	Erledigt
1	Für die Datenbearbeitung verantwortliches öffentliches Organ (Kontaktdaten) – Vollständige Anschrift – Telefonnummer – Website – E-Mail Adresse – Social Media – Weitere relevante Informationen	☐
2	Bearbeitete Personendaten (Datenerhebung für den Download der App, bei der Nutzung der App)	☐
3	Rechtsgrundlage für die Datenbearbeitung	☐
4	Zweck der Datenbearbeitung (detaillierte Zusammenstellung, wofür welche Personendaten bearbeitet werden)	☐
5	Zugriff auf Personendaten auf dem Gerät (welche Zugriffsberechtigungen erteilt die Nutzerin oder der Nutzer mit dem Download bzw. mit der Zustimmung zu den Nutzungsbedingungen dem öffentlichen Organ) – mit Begründung: ■ Aktivitätsdaten: Begründung ■ Bluetooth-Freigabe: Begründung ■ Erinnerungen: Begründung ■ Facebook: Begründung ■ Fotos: Begründung ■ Kalender: Begründung ■ Kamera: Begründung ■ Kontakte: Begründung ■ Körpersensoren: Begründung ■ Mikrofon: Begründung ■ Ortungsdienste: Begründung ■ SMS: Begründung ■ Speicher: Begründung ■ Standort: Begründung ■ Telefon: Begründung ■ Twitter: Begründung	☐

Nr.	Checklisten Punkt	Erledigt
	Beispiele: ■ *Netzwerkkommunikation: Der Zugriff auf das Internet ist erforderlich, um Mails zu versenden oder Links auf externe Websites zu öffnen.* ■ *Speicher: Der Zugriff auf den Speicher ist nötig, um PDFs speichern zu können.* ■ *Kamera: Der Zugriff auf die Kamera wird benötigt, wenn für die Nutzung der Funktionen «Auskunftsrecht» und «Reporter» Bilder von Dokumenten mitgeschickt werden sollen.*	
6	Getroffene organisatorisch-technische Massnahmen zur Gewährleistung der Schutzziele	☐
7	Einbezug Dritter im Sinne eines Outsourcings	☐
8	Weitergabe von Personendaten an Dritte	☐
9	Aufbewahrungsdauer und Löschungsmechanismen der mit der App bearbeiteten Personendaten	☐
10	Die für die Rechte der Nutzerinnen und Nutzer zuständige Stelle und Ansprechperson (Auskunftsrecht, Berichtigung und Löschung von Personendaten)	☐
11	Speicherort der Personendaten (Serverstandort)	☐

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh