LEHRSTUHL FÜR RECHT UND SICHERHEIT DER DIGITALISIERUNG

TECHNISCHE UNIVERSITÄT MÜNCHEN

Praxisworkshop Datenschutz für StartUps

Rechtliche Prüfung des Geschäftsmodel

Thua Duc Nguyen

Inhaltsverzeichnis

Abstract

Das Projekt zielt auf die Entwicklung einer innovativen Finanzmanagement-Plattform ab, die individuellen Nutzern ermöglicht, ihre finanziellen Angelegenheiten effizienter zu verwalten und finanzielle Ziele zu erreichen. Kernfunktionen umfassen die Verfolgung von Einnahmen und Ausgaben für einen transparenten Überblick über die finanzielle Lage, KI-unterstützte Budgetplanung und -analyse für optimierte Ausgabenkontrolle, Spar- und Investitionsmanagement zur Förderung intelligenter Finanzentscheidungen, Werkzeuge zum Schuldenabbau für eine reduzierte finanzielle Belastung und die Möglichkeit, finanzielle Ziele zu setzen und deren Erreichung in Echtzeit zu verfolgen. Diese Plattform verspricht eine ganzheitliche Lösung für das persönliche Finanzmanagement, die Nutzern hilft, ihre finanziellen Ressourcen besser zu organisieren und langfristige finanzielle Stabilität zu sichern.

1 Verarbeitung personenbezogener Daten unter Berücksichtigung von Art. 9 Abs. 1 DS-GVO

Das Geschäftsmodell der „Finance Management App“ konzentriert sich auf die Entwicklung einer Plattform für das persönliche Finanzmanagement. Diese unterstützt Privatpersonen dabei, ihre finanzielle Situation zu managen und ihre finanziellen Ziele zu erreichen. Zu den Hauptfunktionen gehören die Verfolgung von Einnahmen und Ausgaben, KI-gestützte Budgetplanung und -analyse, Spar- und Investitionsmanagement sowie die Verfolgung finanzieller Ziele. Die Verarbeitung personenbezogener Daten ist für die Funktionen der Plattform, die es Einzelpersonen ermöglichen, ihre finanzielle Situation zu verwalten und finanzielle Ziele zu erreichen, von zentraler Bedeutung. Im Rahmen der Anwendung werden folgende Arten von Daten verarbeitet

1. **Personenbezogene Daten:** Um ein Konto einzurichten und die Plattform personalisiert nutzen zu können, werden Informationen wie Name, E-Mail-Adresse und Alter des Nutzers verarbeitet.

2. **Finanzielle Informationen:** Dazu gehören Daten über Einnahmen, Ausgaben und Investitionen. Die Daten werden benötigt, um den Nutzern einen Überblick über die finanzielle Situation zu geben.

3. **Nutzungsdaten und Interaktionsdaten mit der Plattform:** Dazu gehören Daten darüber, welche Funktionen sie nutzen und wie sie mit der Plattform interagieren. Diese Informationen sind wichtig, um die Nutzererfahrung zu verbessern.

Ob es sich um sensible personenbezogene Daten im Sinne von Art. 9 Abs. 1 DS-GVO handelt, hängt davon ab, ob Daten verarbeitet werden, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie ob es sich um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung handelt.

Bei der primären Datenerhebung und -verarbeitung handelt es sich nicht unmittelbar um die Erhebung sensibler personenbezogener Daten im Sinne von Art. 9 DS-GVO. Die detaillierte Analyse finanzieller Transaktionen und Verhaltensweisen könnte jedoch indirekt sensible Informationen offenbaren, beispielsweise durch Rückschlüsse auf Gesundheitsausgaben, politische Spenden oder Mitgliedsbeiträge an Gewerkschaften und religiöse Gruppen. Daher ist es wichtig, dass bei der Entwicklung und dem Betrieb der Plattform strenge Datenschutzrichtlinien und Sicherheitsmaßnahmen umgesetzt werden, um die Privatsphäre der Nutzer zu schützen und die Einhaltung der DS-GVO zu gewährleisten.

2 Verarbeitungsvorgänge personenbezogener Daten in der Plattform

Die Verarbeitung personenbezogener Daten durch die Plattform für das persönliche Finanzmanagement umfasst verschiedene Vorgänge, die in bestimmten Situationen während des Ablaufs der IT-Anwendung stattfinden. Hier sind die konkreten Verarbeitungsvorgänge detailliert beschrieben:

1. **Erhebung von Daten:** Beim Erstellen eines Kontos auf der Plattform werden persönliche Identifikationsinformationen wie Name und E-Mail-Adresse erhoben. Finanzielle Informationen werden erhoben, wenn Nutzer ihre Einnahmen, Ausgaben, Budgets und Investitionsdaten manuell eingeben oder wenn diese Informationen automatisch aus verknüpften Finanzkonten importiert werden.

2. **Speicherung von Daten:** Alle erfassten Daten werden auf sicheren Servern gespeichert, um die Nutzung der Plattformfunktionen zu ermöglichen. Finanzielle Ziele und Fortschrittsdaten der Nutzer werden ebenfalls gespeichert, um die Verfolgung und Analyse des finanziellen Fortschritts zu ermöglichen.

3. **Analyse von Daten:** Die Plattform nutzt KI-gestützte Technologien, um Budgetplanung und -analyse anzubieten. Dabei werden die finanziellen Daten der Nutzer analysiert, um personalisierte Empfehlungen und Einsichten zu bieten. Ausgabenmuster und Investitionen werden analysiert, um Spar- und Investitionsempfehlungen abzuleiten.

4. **Veränderung von Daten:** Nutzer haben die Möglichkeit, ihre persönlichen und finanziellen Daten jederzeit zu aktualisieren oder zu korrigieren, um ihre finanzielle Situation genau widerzuspiegeln.

5. **Löschung von Daten:** Auf Anfrage der Nutzer können persönliche Daten gelöscht werden, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Daten werden auch gelöscht, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind oder wenn das Nutzerkonto gelöscht wird.

Jeder dieser Verarbeitungsvorgänge ist entscheidend für die Funktionalität der Plattform und muss unter strikter Einhaltung von Datenschutzgesetzen und -best practices durchgeführt werden. Besonders wichtig ist dabei die Gewährleistung der Datensicherheit und -integrität, die Verschlüsselung von Daten, der Schutz vor unbefugtem Zugriff und die transparente Kommunikation mit den Nutzern über die Nutzung ihrer Daten.

3 Rechtsgrundlagen für die Verarbeitungsvorgänge auf der Plattform

Für die Verarbeitungsvorgänge personenbezogener Daten in der Finanzmanagement-Plattform können verschiedene Rechtsgrundlagen gemäß der Allgemeinen Datenschutzverordnung (DSGVO) oder entsprechenden lokalen Datenschutzgesetzen herangezogen werden. Hier sind Beispiele für Rechtsgrundlagen für die genannten Verarbeitungsvorgänge:

1. **Einwilligung (Art. 6 Abs. 1 lit. a DSGVO):** Die Nutzer geben ihre ausdrückliche Einwilligung zur Verarbeitung ihrer persönlichen und finanziellen Daten bei der Registrierung auf der Plattform und beim manuellen Eingeben oder Importieren ihrer Finanzdaten. Die Einwilligung umfasst spezifische Verarbeitungsvorgänge wie die Analyse finanzieller Daten für personalisierte Empfehlungen. Nutzer haben das Recht, ihre Einwilligung jederzeit zu widerrufen.

2. **Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Die Verarbeitung personenbezogener Daten ist notwendig, um den mit den Nutzern geschlossenen Vertrag über die Nutzung der Finanzmanagement-Plattform zu erfüllen. Dies beinhaltet die Verarbeitung von Daten zur Kontoerstellung, Budgetplanung, Spar- und Investitionsmanagement sowie zum Schuldenabbau.

3. **Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO):** In einigen Fällen kann die Verarbeitung personenbezogener Daten erforderlich sein, um rechtlichen Verpflichtungen nachzukommen, z.B. bei gesetzlich vorgeschriebenen Finanzberichten oder im Rahmen von Betrugsbekämpfungsmaßnahmen.

4. **Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DSGVO):** Dieser Grund ist weniger relevant für die Finanzmanagement-Plattform, könnte aber in bestimmten Szenarien zur Anwendung kommen, z.B. wenn die Verarbeitung personenbezogener Daten notwendig ist, um lebenswichtige Interessen der Nutzer oder einer anderen natürlichen Person zu schützen.

Jeder dieser Verarbeitungsvorgänge erfordert eine spezifische Rechtsgrundlage, die je nach Kontext der Datenverarbeitung und der Art der personenbezogenen Daten ausgewählt wird. Wichtig ist, dass die Plattform die entsprechende Rechtsgrundlage klar dokumentiert und den Nutzern transparent kommuniziert, auf welcher Basis ihre Daten verarbeitet werden.

4 Rollen und Verantwortlichkeiten in der Datenverarbeitung der Plattform

Basierend auf der Struktur DES Projekte und den Anforderungen der DSGVO können folgende Annahmen getroffen werden:

1. **Verantwortlicher:** Der Verantwortliche ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Kontext des beschriebenen Projekts wäre dies typischerweise das Unternehmen oder die Organisation, die die Finanzmanagement-Plattform initiiert und betreibt. Sie sind verantwortlich für die Einhaltung der Datenschutzgesetze und müssen sicherstellen, dass alle Verarbeitungstätigkeiten der personenbezogenen Daten im Einklang mit der DSGVO stehen.

2. **Auftragsverarbeiter:** Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. In der Entwicklung und dem Betrieb einer solchen Plattform könnten externe Dienstleister als Auftragsverarbeiter eingesetzt werden, z.B. für Cloud-Hosting, Datenanalyse, Kundensupport oder Finanzdienstleistungen. Der Einsatz von Auftragsverarbeitern erfordert einen Vertrag oder eine andere rechtliche Grundlage, die den Auftragsverarbeiter zur Einhaltung der DSGVO und zum Schutz der personenbezogenen Daten verpflichtet.

3. **Eigene Rolle als Auftragsverarbeiter:** Falls das Unternehmen oder die Organisation, die das Projekt durchführt, personenbezogene Daten im Auftrag eines anderen Unternehmens oder einer anderen Organisation verarbeitet (z.B. wenn es als Anbieter von Finanzmanagement-Lösungen für Banken oder andere Finanzinstitutionen fungiert), würde es selbst als Auftragsverarbeiter agieren. In diesem Fall müsste es die Anforderungen der DSGVO für Auftragsverarbeiter erfüllen, einschließlich der Verarbeitung von Daten gemäß den Anweisungen des Verantwortlichen und der Implementierung angemessener technischer und organisatorischer Maßnahmen zum Schutz der Daten.

Es ist entscheidend, dass die Rollen und Verantwortlichkeiten im Zusammenhang mit der Datenverarbeitung klar definiert und dokumentiert werden, um die Einhaltung der Datenschutzgesetze zu gewährleisten. Die Verantwortlichen müssen auch die Transparenz gegenüber den betroffenen Personen sicherstellen, indem sie sie über die Verarbeitung ihrer Daten, die Identität des Verantwortlichen und gegebenenfalls des Auftragsverarbeiters informieren.

5 Implementierte Datenschutzmaßnahmen und deren Bewertung für die Plattform

Basierend auf Best Practices und den Anforderungen der Datenschutz-Grundverordnung (DSGVO) kann eine Reihe von Maßnahmen identifiziert werden, die typischerweise implementiert werden sollten, um den Datenschutz und die Datensicherheit zu gewährleisten. Außerdem werde ich beurteilen, ob diese Maßnahmen ausreichen oder ob zusätzliche Maßnahmen erforderlich sein könnten.

1. **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy by Design and by Default):** Implementierung von Verschlüsselungstechnologien für Datenübertragungen (z.B. TLS/SSL) und für gespeicherte Daten (z.B. AES). Begrenzung der Datenerhebung, -speicherung und -zugriffe auf das für die spezifischen Zwecke notwendige Minimum. Automatische Löschung oder Anonymisierung nicht mehr benötigter Daten.

2. **Zugangskontrollen:** Einsatz von starken Authentifizierungsverfahren für Nutzerzugänge, einschließlich Multi-Faktor-Authentifizierung. Definition von Berechtigungen auf Basis der geringsten Rechte (Prinzip der minimalen Rechte).

3. **Datensicherheit:** Einsatz von Firewalls und anderen Netzwerksicherheitstechnologien zur Abwehr externer Angriffe. Regelmäßige Sicherheitsüberprüfungen und Penetrationstests, um Schwachstellen zu identifizieren und zu beheben.

4. **Datenschutz-Folgenabschätzung und regelmäßige Überprüfung:** Durchführung von Datenschutz-Folgenabschätzungen für Verarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Regelmäßige Überprüfung und Aktualisierung der Datenschutzpraktiken und -maßnahmen.

5. **Schulung und Bewusstseinsbildung:** Schulung der Mitarbeiter in Datenschutzpraktiken und -richtlinien. Sensibilisierung für Datenschutzrisiken und für den richtigen Umgang mit personenbezogenen Daten.

6. **Verfahren zur Reaktion auf Datenschutzverletzungen:** Etablierung eines Prozesses für die Meldung und Behebung von Datenschutzverletzungen, einschließlich der Benachrichtigung der zuständigen Aufsichtsbehörde und der betroffenen Personen.

Ob diese Maßnahmen ausreichen, hängt von einer kontinuierlichen Bewertung der Risiken und der Effektivität der implementierten Schutzmaßnahmen ab. Es ist wichtig, dass das

Projektmanagement die sich ständig weiterentwickelnden Bedrohungen und Technologien im Auge behält und die Maßnahmen entsprechend anpasst. Zusätzliche Maßnahmen könnten notwendig sein, um neue Risiken zu adressieren oder um auf Feedback von Nutzern oder Änderungen in den rechtlichen Anforderungen zu reagieren.

6 Wesentliche Informationspflichten nach DSGVO für Nutzer der Finanzmanagement-Plattform

Gemäß der Datenschutz-Grundverordnung (DSGVO) sind Sie verpflichtet, den betroffenen Personen eine Reihe von wesentlichen Informationen bezüglich der Verarbeitung ihrer personenbezogenen Daten mitzuteilen. Im Kontext des Projekts zur Entwicklung einer Plattform für das persönliche Finanzmanagement sollten folgende Informationen den Nutzern klar und verständlich kommuniziert werden:

1. **Identität und Kontaktdaten des Verantwortlichen:** Den Nutzern muss mitgeteilt werden, wer für die Verarbeitung ihrer personenbezogenen Daten verantwortlich ist. Dies umfasst den Namen und die Kontaktdaten des Unternehmens oder der Organisation sowie gegebenenfalls des Datenschutzbeauftragten.

2. **Zwecke der Datenverarbeitung:** Es muss klar angegeben werden, für welche spezifischen Zwecke die personenbezogenen Daten verarbeitet werden (z.B. Budgetverwaltung, Spar- und Investitionsplanung).

3. **Rechtsgrundlage der Verarbeitung:** Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten muss den Nutzern mitgeteilt werden (z.B. Verarbeitung aufgrund der Einwilligung der Nutzer, zur Vertragserfüllung oder aufgrund eines berechtigten Interesses).

4. **Empfänger oder Kategorien von Empfängern der personenbezogenen Daten:** Falls die Daten an Dritte weitergegeben werden, sollten die Nutzer darüber informiert werden, wer diese Empfänger sind oder welche Kategorien von Empfängern existieren (z.B. Auftragsverarbeiter, Finanzdienstleister).

5. **Datenübermittlung an ein Drittland oder eine internationale Organisation:** Wenn Daten außerhalb der EU/EWR übermittelt werden, muss dies angegeben werden, zusammen mit den Sicherheitsmaßnahmen, die zum Schutz der Daten ergriffen wurden.

6. **Dauer der Speicherung der personenbezogenen Daten:** Die Nutzer müssen darüber informiert werden, wie lange ihre Daten gespeichert werden oder welche Kriterien für die Festlegung dieser Dauer angewendet werden.

7. **Rechte der betroffenen Personen:** Den Nutzern müssen ihre Rechte in Bezug auf ihre Daten mitgeteilt werden, einschließlich des Rechts auf Zugang, Berichtigung, Löschung

(„Recht auf Vergessenwerden“), Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch gegen die Verarbeitung.

8. **Das Recht auf Widerruf der Einwilligung:** Wenn die Verarbeitung auf der Einwilligung basiert, sollte den Nutzern mitgeteilt werden, dass sie das Recht haben, ihre Einwilligung jederzeit zu widerrufen, ohne dass dies die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt.

9. **Das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen:** Die Nutzer sollten darauf hingewiesen werden, dass sie das Recht haben, eine Beschwerde bei einer Datenschutzaufsichtsbehörde einzureichen, wenn sie der Meinung sind, dass die Verarbeitung ihrer personenbezogenen Daten gegen die DSGVO verstößt.

Diese Informationen sollten den Nutzern zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten in einer klaren, transparenten und leicht zugänglichen Form zur Verfügung gestellt werden.