LEHRSTUHL FÜR RECHT UND SICHERHEIT DER DIGITALISIERUNG

TECHNISCHE UNIVERSITÄT MÜNCHEN

Praxisworkshop Datenschutz für StartUps

Rechtliche Prüfung des Geschäftsmodel

Thua Duc Nguyen

Inhaltsverzeichnis

Abstract

Ziel des Projektes ist die Entwicklung einer innovativen Finanzmanagementplattform, die es einzelnen Nutzern ermöglicht, ihre finanziellen Angelegenheiten effizienter zu verwalten und finanzielle Ziele zu erreichen. Kernfunktionen sind die Verfolgung von Einnahmen und Ausgaben für einen transparenten Überblick über die finanzielle Situation, KI-gestützte Budgetplanung und -analyse zur optimierten Ausgabenkontrolle, Spar- und Anlagemanagement zur Förderung intelligenter Finanzentscheidungen und die Möglichkeit, finanzielle Ziele zu setzen und deren Erreichung in Echtzeit zu verfolgen.

Die rechtliche Prüfung des Projekts erfordert eine detaillierte Analyse verschiedener Aspekte. Dazu gehört die Ermittlung der personenbezogenen Daten einschließlich der sensiblen Daten sowie die Beschreibung der konkreten Verarbeitungsvorgänge. Es ist wichtig, die Rechtsgrundlagen für jede Verarbeitungstätigkeit zu prüfen und sicherzustellen, dass diese auf einer gültigen Rechtsgrundlage beruhen, sei es durch die Einwilligung der betroffenen Personen oder durch eine Interessenabwägung. Darüber hinaus muss der für die Verarbeitung Verantwortliche eindeutig bestimmt werden und es muss geprüft werden, ob Auftragsverarbeiter beteiligt sind. Des Weiteren sind die bereits getroffenen technisch-organisatorischen Maßnahmen zur Einhaltung der Datenschutzgrundsätze auf ihre Angemessenheit hin zu überprüfen und gegebenenfalls ergänzende Maßnahmen zu treffen. Schließlich ist es wichtig, die wesentlichen Informationen, die den betroffenen Personen über die Datenverarbeitung mitgeteilt werden müssen, klar zu definieren, um Transparenz und die Einhaltung der Datenschutzvorschriften zu gewährleisten.

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, die 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, finanzielle Ziele und Plannen. Die Daten werden für die Kernfunktionen der Plattformdienste benötigt.

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

Um die Verarbeitungsvorgänge gemäß der in der Anfrage beschriebenen Aktivitäten auf einer rechtlichen Basis nach der DS-GVO zu rechtfertigen, können wir auf Artikel 6 der DS-GVO zurückgreifen. Hier ist, wie jeder Verarbeitungsvorgang gerechtfertigt werden kann:

1. **Datenerhebung:** Dies kann auf Basis der Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 a DS-GVO gerechtfertigt werden, da die Nutzer aktiv ihre persönlichen und finanziellen Informationen bereitstellen. Darüber hinaus kann die Erfassung finanzieller Daten für die Vertragsdurchführung (Nutzung der Plattformdienste) erforderlich sein, was eine Rechtfertigung nach Art. 6 Abs. 1 b DS-GVO darstellt.

2. **Speicherung der Daten:** Die Speicherung von Daten kann aufgrund der Notwendigkeit für die Erfüllung eines Vertrags (Art. 6 Abs. 1 b DS-GVO) gerechtfertigt werden, insbesondere um den Nutzern die Nutzung der Plattformfunktionen zu ermöglichen.

3. **Analyse der Daten:** Die Nutzung von KI zur Budgetplanung und -analyse fällt unter die Kategorie der Vertragsdurchführung (Art. 6 Abs. 1 b DS-GVO), da sie direkt mit den angebotenen Dienstleistungen der Plattform zusammenhängt.

4. **Änderung der Daten:** Das Recht der Nutzer, ihre Daten zu aktualisieren oder zu korrigieren, kann als Teil der Vertragserfüllung (Art. 6 Abs. 1 b DS-GVO) gesehen werden, sowie durch die Einwilligung der betroffenen Person (Art. 6 Abs. 1 a DS-GVO).

5. **Löschung von Daten:** Die Löschung von Daten auf Anfrage der Nutzer kann auf die Einwilligung gemäß Art. 6 Abs. 1 a DS-GVO gestützt werden, insbesondere wenn die Datenverarbeitung nicht mehr notwendig ist oder wenn der Nutzer seine Einwilligung widerruft

In jedem Fall ist es wichtig, dass die Einwilligung der betroffenen Person spezifisch, informiert und eindeutig ist, um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten. Bei einer Verarbeitung aufgrund berechtigter Interessen muss außerdem eine sorgfältige Interessenabwägung vorgenommen werden, um sicherzustellen, dass die Rechte und Freiheiten der betroffenen Person nicht überwiegen.

4 Rollen und Verantwortlichkeiten in der Datenverarbeitung der Plattform

Im Kontext der DS-GVO wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter unterschieden. Gemäß Art. 28 DS-GVO ist der Verantwortliche die Person oder Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Auftragsverarbeiter hingegen ist eine Person oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- **Wer ist der Verantwortliche?** In Bezug auf das Projekt wäre der Verantwortliche das Unternehmen, die die Plattform betreibt. Dieses Unternehmen entscheidet über die Zwecke (z.B. die Bereitstellung von Dienstleistungen zur Finanzverwaltung) und die Mittel (z.B. die technischen Lösungen und Prozesse) der Datenverarbeitung.
- **Einsatz von Auftragsverarbeitern** Das Unternehmen könnte zur Unterstützung bestimmter Funktionen der Plattform oder zur Speicherung der Daten Auftragsverarbeiter einsetzen. Beispiele für Auftragsverarbeiter könnten Cloud-Dienstanbieter, Anbieter von Kundenbetreuungssoftware oder Dienstleister für die Datenanalyse sein.
- **Verantwortung bei Einsatz von Auftragsverarbeitern** Gemäß Art. 28 DS-GVO muss der Verantwortliche sicherstellen, dass Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, um einen Datenschutz gemäß den Anforderungen der DS-GVO zu gewährleisten. Der Verantwortliche und der Auftragsverarbeiter müssen einen Vertrag abschließen, der den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt.

  Wichtig ist auch, dass Auftragsverarbeiter nur auf dokumentierte Weisung des Verantwortlichen handeln dürfen und die personenbezogenen Daten nicht für eigene Zwecke verwenden dürfen. Verstößt ein Auftragsverarbeiter gegen diese Vorgaben, indem er über die Zwecke und Mittel der Verarbeitung entscheidet, gilt er gemäß der DS-GVO als Verantwortlicher in Bezug auf diese Verarbeitung.

5 Implementierte Datenschutzmaßnahmen und deren Bewertung für die Plattform

Basierend auf den Anforderungen der Art. 5 Abs. 1 f DS-GVO kann eine Reihe von Maßnahmen identifiziert werden, die typischerweise implementiert werden sollten, um den Datenschutz und die Datensicherheit zu gewährleisten.

1. **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:** Implementierung von Verschlüsselungstechnologien für Datenübertragungen (z.B. TLS/SSL) und für gespeicherte Daten. 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.

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 DS-GVO für Nutzer der Plattform

Im Kontext des Projekts sollten folgende Informationen den Nutzern klar und verständlich kommuniziert werden:

1. **Verantwortlicher und Datenschutzbeauftragter (Art. 13 Abs. 1 a-b DS-GVO):** Name und Kontaktdaten des Verantwortlichen (und gegebenenfalls seines Vertreters) sowie die Kontaktdaten des Datenschutzbeauftragten.
2. **Zwecke und Rechtsgrundlage der Verarbeitung (Art. 13 Abs. 1 c, Art. 14 Abs. 1 c DS-GVO):** Die spezifischen Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, und die Rechtsgrundlage der Verarbeitung müssen klar definiert werden.
3. **Berechtigte Interessen (Art. 13 Abs. 1 d DS-GVO):** Falls die Verarbeitung auf berechtigten Interessen beruht, sind diese dem Betroffenen mitzuteilen.
4. **Empfänger oder Kategorien von Empfängern (Art. 13 Abs. 1 e DS-GVO):** Die Identität von Empfängern oder die Kategorien von Empfängern, denen die Daten offengelegt wurden oder werden.
5. **Datenübermittlung (Art. 13 Abs. 1 f DS-GVO):** Informationen über die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation sowie die Vorkehrungen zum Schutz der Daten.
6. **Speicherdauer (Art. 13 Abs. 2 a DS-GVO):** Die geplante Dauer der Speicherung der personenbezogenen Daten oder die Kriterien zur Festlegung dieser Dauer.
7. **Rechte der betroffenen Person (Art. 13 Abs. 2 b DS-GVO):** Das Recht auf Zugang, Berichtigung, Löschung der Daten, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung, und das Recht auf Datenübertragbarkeit.
8. **Widerrufsrecht (Art. 13 Abs. 2 c DS-GVO):** Das Recht, eine Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der Verarbeitung, die auf der Einwilligung vor ihrem Widerruf beruht, beeinträchtigt wird.
9. **Beschwerderecht (Art. 13 Abs. 2 d DS-GVO):** Das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

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