Datenschutz und Datensicherheit

Delegator

|  |  |
| --- | --- |
| Klassifizierung | intern |
| Status | in Arbeit |
| Programmname | Delegator |
| Projektnummer | 1 |
| Projektleiter | Tabinas Kenan |
| Version | 1 |
| Datum | 06. Juni 2025 |
| Auftraggeber | Tabinas Kenan |
| Autor/Autoren | Tabinas Kenan |
| Verteiler |  |

Änderungsverzeichnis

| Version | Datum | Änderung | Autor |
| --- | --- | --- | --- |
| 1 | 06.06 | Erstellt | TAK |

Tabelle : Änderungsverzeichnis

# Übersicht und Zweck

Es folgt ein Managementsummary. Damit ein gemeinsames Verständnis gegenüber der Applikation und dessen Inhalt aufgebaut werden kann.

## Management Summary

## Zweck dieses Konzeptes

Es ist nicht nur etwaige datenschutzrechliche Anforderungen zu erfüllen wie z.B. die der DSGVO oder das Schweizerische Datenschutzgesetzt (nDSG).

Sondern auch die Daten der Kunden zu Respektieren. Es besteht die Möglichkeit das die Applikation Informationen von Persönlichkeiten der Öffentlichkeit verwendet wird. Es ist im gemeinsamen Interesse, das diese Daten mit höchster Sorgfalt behandelt werden.

# Rechtliche Grundlagen

## Bestehendes Recht

Folgende Bereits erwähnte Rechtsgrundlagen sind bereits in Kraft. Dabei beschränken wir uns auf den DACH (Deutschland, Austria, Schweiz) Raum.

* DSGVO: Allen EU-Bürgern
* nDSG: Allen Schweizern-Bürgern

## Verantwortlichkeiten

* Delegator: Kenan Tabinas
* Service: CaaS Provider

## Wichtigkeit

Jetzt stellt sich die Frage: Wieso ist das für uns Relevant.

* Aus Respekt gegenüber dem Kunden
* DSVGO-Busgelder bis zu 4% des Jahreseinkommen.[[1]](#footnote-1)
* nDSG-Busgelder bis zu 250'000 CHF.[[2]](#footnote-2)
* Ein Muss für Investoren[[3]](#footnote-3)

# Datenarten und Zweck

## Personenbezogene Daten

### Stammdaten

* E-Mail-Adresse
* Benutzername
* Passwort (verschlüsselt)
* Profilbild (optional)
* Zugehörigkeit zu Organisation

### Nutzungsdaten

* Termine
* Kalenderdaten
* Aufgaben
* Projekte
* Setlisten
* Songs
* Chat Nachrichten
* Zugriffszeiten (Sicherheit)
* Speicherbedarf (Monitoring von Wachstum)

## Zweck

Alle diese Daten dienen nur der Verfügbarkeit des Dienstes.

Sie sollte nicht für Marketing oder andere Zwecke missbraucht werden.

# Rechtsgrundlagen der Verarbeitung

Ohne die Rechtliche Grundlage

## Art. 6 DSGVO / Art. 13 nDSG

### Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):

* Benutzerkonto-Verwaltung
* Bereitstellung der Kernfunktionen
* Kalender- und Aufgabenverwaltung

### Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):

* Systemsicherheit und Betriebsstabilität
* Fehleranalyse und technische Optimierung
* Schutz vor Missbrauch

### Einwilligung (Art. 6 Abs. 1 lit. a DSGVO):

* Marketing-E-Mails
* Erweiterte Analytics
* Nicht-essenzielle Cookies

Text stammt aus Claude.

# Wiederrufsrecht

Damit die Applikation funktioniert werden gewisse Daten benötigt. Die zwingenden Cookies die man von Webseiten kennt. Man macht sich Strafbar, wenn die Cookies ablehnt und die Applikation nicht mehr funktioniert.

Basierend auf den Aritkel von Zuvor (Art. 6 Abs. 1 lit. b DSGVO und Art. 13 Abs. 2 lit. a nDSG) haben wir für das Projekt eine klare Abgrenzung zwischen vertragserfüllungsrelevanter und einwilligungspflichtiger Datenverarbeitung vorgenommen.

## ****Vertragserfüllung****

### ****Kalenderfunktion****

* Termine speichern Nötig für versprochenen Service
* Erinnerungen senden Teil der Kalenderfunktion
* Mit anderen Bandmitgliedern teilen Kern-Feature

### ****Aufgabenverwaltung****

* Aufgaben erstellen/zuweisen Versprochener Service
* Status-Updates Nötig für Funktionalität
* Benachrichtigungen Teil des Services

### ****Benutzerkonto****

* Name, E-Mail speichern Nötig für Account
* Login-Daten Nötig für Zugang
* Gruppenzugehörigkeit Nötig für Band-Features

## Nicht Vertragserfüllung fällt:

### ****Marketing:****

* Newsletter über neue Features Nicht für Service nötig
* Werbung für andere Produkte Nicht vertraglich vereinbart
* Marktforschung Nicht Teil des Services

### ****Analytics:****

* Detailliertes Nutzerverhalten Nicht nötig für Service
* A/B-Tests Nicht vertraglich vereinbart
* Performance-Optimierung Kann auch ohne erfolgen

Text aus Claude

# Technische Massnahmen

## Wichtigkeit

Ein Leak von Privaten Daten zerstört nicht nur das Vertrauen, Existenzen und kann auch Schadensersatzforderungen kommen.

## Verschlüsselung

* **In Transit**: TLS 1.3 für alle Datenübertragungen
* **At Rest**: AES-256 Verschlüsselung für sensible Daten
* **Passwörter**: bcrypt mit Salt, mindestens 12 Rounds

Vorschläge von Claude.

## Zugriffskontrolle

* Multi-Faktor-Authentifizierung
* Rollenbasierte Zugriffsrechte
* Kurze Timeout Intervalle

## Einstellungen für die Organisation

Folgende Einstellungen könnten in der Organisation gewählt werden. Damit folgende Richtlinien vom Organisation Admin auferlegt wird anstelle vom Unternehmen.

* Multi-Faktor zwingend für alle User der Organisation
* Passwort des Users wird Generiert (Passwort Manager zwang)

# Massnahmen

## US Server

Weshalb ist die Wahl des Cloud Prodivders Relevant? Ich bin kein Jurist, aber laut dem Schermen Urteil II scheint der Fall klar zu sein. Das Schnutzniveau von dem US Privacy Shield nicht ausreichend.

«Mit Urteil vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II“) hat der EuGH diesen Durchführungsbeschluss zum Privacy Shield für unwirksam erklärt.»[[4]](#footnote-4)

«Bezüglich der Standarddatenschutzklauseln (Standardvertragsklauseln) hat der EuGH im Schrems II-Urteil entschieden, dass diese grundsätzlich weiterhin genutzt werden können. Allerdings muss tatsächlich ein Schutzniveau für die personenbezogenen Daten sichergestellt sein, das dem in der Europäischen Union entspricht»[[5]](#footnote-5)

Das heisst nicht Schützenswerte Daten dürfen auch auf US Servern liegen, alle anderen müssen in der mindestens in der EU bleiben.

## US Providers

Leider endet es hier nicht. In den US gilt der CLOUD Act. US Behörden können die Herausgabe von Daten von Unternehmen mit Sitz in USA fordern. Dies trift auch zu wenn die Server in beispielsweise in der Schweiz liegen.

«Datenschutz-Experten sehen hier einen klaren Konflikt mit der Datenschutzgrundverordnung, die Unternehmen die Übergabe von innerhalb der EU gesicherten Daten ohne Rechtshilfeabkommen verbietet (vgl. Artikel 48 DSGVO). Ein Verstoß gegen die in Artikel 48 aufgeführten Pflichten kann nach Art. 83 DSGVO mit Bußgeldern in Höhe von bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Jahresumsatzes geahndet werden.»[[6]](#footnote-6)

## Kalender Integration

Bei der Verwendung von Kalender Integration wie z.B. Google Calender muss auch darauf geachtet werden, das möglich wenig Daten übertragen werden.

# Betroffennenrecht

Das Betroffenenrecht, anders als ich gedacht habe, hat nichts mit Verstorbenen zu tun. Sondern beschreibt Rechte, welche ich habe, wenn ich in der EU meine Daten einem Unternehmen gebe.

## Auskunftsrecht

Alle Daten müssen jeder Zeit einsehbar sein.

«Mit dem Auskunftsrecht garantiert Ihnen Art. 15 der Datenschutz-Grundverordnung (DSGVO) ein bedeutsames Betroffenenrecht. Danach können Sie als betroffene Person von dem für die Datenverarbeitung Verantwortlichen Auskunft darüber verlangen, welche Daten dort über Sie gespeichert sind bzw. verarbeitet werden.» [[7]](#footnote-7)

## Recht auf Berchtigung

Alle Daten müssen jeder Zeit änderbar sein.

«Das Recht auf Berichtigung ist sehr klar und schnell zusammengefasst: Wenn Ihnen auffallen sollte, dass Sie betreffende Daten unrichtig sind, so können Sie deren unverzügliche Berichtigung verlangen.»[[8]](#footnote-8)

## Einschränkung auf Verarbeitung

Der Account muss einfrierbar / deaktivierbar sein.

«Während der Einschränkung dürfen Ihre Daten nur noch gespeichert, aber nicht mehr auf andere Weise verarbeitet werden. Die Einschränkung dient dazu, Ihre Rechte in Ausgleich mit den Rechten des für die Verarbeitung Verantwortlichen zu bringen.»

## Recht auf Vergessenwerden

Der User hat recht das seine Daten gelöscht werden.

«Das Recht auf Löschung ist eines der zentralen Werkzeuge zur Durchsetzung Ihrer datenschutzrechtlichen Selbstbestimmung. Mit diesem Recht können Sie die restlose Entfernung Ihrer personenbezogenen» [[9]](#footnote-9)

Dabei gibt es eine Ausnahme, wenn ich z.B. die Aufbewahrungspflicht für Steuererklärung.

«Nach Art. 17 Abs. 3 DSGVO gibt es Ausnahmen vom Recht auf Löschung, die direkt in der DSGVO geregelt sind Betroffenenrechte der DSGVO - Das Recht auf Löschung / "Recht auf Vergessenwerden" (Art. 17 DSGVO). Eine wichtige Ausnahme ist, wenn andere Rechtsvorschriften eine Aufbewahrung verlangen.»

# Incident Response

## Datenschutzverletzungen

### Erkennungsmaßnahmen

* **Monitoring**: Automatische Erkennung ungewöhnlicher Zugriffe
* **Logging**: Umfassende Protokollierung sicherheitsrelevanter Ereignisse
* **Alerting**: Sofortige Benachrichtigung bei kritischen Ereignissen

### Response-Prozess

* **Sofortmaßnahmen**: Eindämmung der Verletzung (binnen 1 Stunde)
* **Bewertung**: Risikoanalyse und Betroffenen-Impact (binnen 4 Stunden)
* **Meldung**: An Aufsichtsbehörde binnen 72 Stunden
* **Benachrichtigung**: Der Betroffenen bei hohem Risiko
* **Dokumentation**: Vollständige Aufzeichnung des Vorfalls

## Meldeverfahren

* **Interne Meldung**: Klare Eskalationswege
* **Behördenmeldung**: Template für einheitliche Meldungen
* **Betroffenen-Information**: Verständliche Kommunikation

Erstellt von Claude

# Roadmap

## Grundlagen

Zeitraum: Monat 1-2

* Datenschutzerklärung erstellen
* Cookie-Consent-System implementieren
* Grundlegende Sicherheitsmaßnahmen
* Betroffenenrechte-Interface

## Erweiterte Massnahmen

Zeitraum: Monat 3-4

* Verschlüsselung at Rest implementieren
* Audit-Logging einrichten
* Incident Response Prozesse
* Mitarbeiter-Schulungen

## Optimierung

Zeitraum: Monat 5-6

* Automatisierte Löschung
* Erweiterte Analytics (privacy-compliant)
* Penetration Testing
* Compliance-Review

# Fazit

## Weniger ist mehr

Weniger ist mehr. Also nein weniger ist nie mehr. Aber weniger Daten zu sammeln hat mehrere Vorteile:

* Weniger Speicherplatz
* Weniger Verpflichtungen

## Rechte

Jeder User muss folgende Rechte haben:

* Recht auf Dateneinsicht
* Recht auf Deaktivierung
* Recht auf Vergessenwerden

## Verantwortung

Ich bin verpflichtet die Daten zu schützen.

* Monitoring
* Logging
* Alarmierung
* Pentesting

## Reaktion

Sobald etwas passiert ist muss ich folgende Schritte Einleiten:

* Sofortmassnahmen
* Betroffenen User Informieren
* Behörden Informieren
* Dokumentieren

## Zeitplan

Damit diese nicht gewinneinbringenden Massnahmen nichts in Vergessenheit geraten und geschäftsschädigend werden ist es wichtig einen Plan zu haben.

### Vor der Veröffentlichung

* Kurzfristig ist unteranderem folgende Punkte zu beachten:
* Oberfläche, um Rechte auszuüben
* AGB erstellen
* Sicherheitsmassnahmen
* Rechtskonformer Cloud Provider finden

## Zukunft

Langfristig sind unteranderem folgende Punkte zu beachten:

* Datenschutz Audit mit Externen
* Penetration Test von Externen
* Incidents Report Tests
* Datenschutz Themen im Budget einplanen

Abkürzungen und Glossar

| Abkürzung /  Fachwort | Erläuterung |
| --- | --- |
| DSGVO | Datenschutzgrundverordnung |
| nDSG | National (Schweiz) Datenschutz Gesetz |
| DACH | (Deutschland, Austria, Schweiz) |
| bcrypt | Eine Art Passwort hashing. |
| API | Steht für Application Programming Interface. Ist eine Schnittstelle, die in Form von Endpoints, Daten via JSON bereitstellen oder verarbeiten. |
| Bearer Token | Theoretisches Konzept für Authentifizierung in diesem Fall umgesetzt mit JWT in Django |
| Django REST | Ein Framework zur Erweiterung Django für die Entwicklung von REST-APIs |
| Docker | Plattform für bereitstellen von Container. Ähnlich wie ein VMWare aber für Container anstelle von Containern. |
| Flutter | Crossplattform Framework. Analog zu .Net Maui und React Native |
| Gunicorn | Python HTTP Server. Als Brücke zwischen Django und nginx. |
| Hot-Reload | Ermöglicht Neuladen von Code-Änderungen ohne Neustart |
| IoT | Steht für Internet of Things. Beispiel Kühlschrank, welcher dir sagt, was du noch zuhause hast. |
| JWT | Steht für JSON Web Token. Ist ein Alphanumerischer Code, welcher bei der Authentifizierung genutzt wird. |
| Wireframe | Visueller Entwurf einer Benutzeroberfläche. Verglichen zum Mockup keine Farbe und keine Bilder. |
| Postman | Software zum Testen und Entwickeln von APIs. In diesem Fall als VS Code Exention. |
| Raspberry Pi (Raspi) | Singleboardcomputer. In diesem Fall Raspi 5. |

Tabelle : Glossar 1

Vorschläge der Wörter kommen von Claude. Erläuterungen nicht.

| Abkürzung / Fachwort | Erläuterung |
| --- | --- |
| CLOUD Act | US Gesetz Behörden den Zugriff auf Daten von US-Unternehmen ermöglicht. |
| Schrems II | Urteil vom EU-Parlament von 2020. In dem wurde Privacy Shield als ungültig erklärt. |
| Privacy Shield | Ehemaliges Datenschutzabkommen zwischen EU und USA. |
| Standardvertragsklauseln | Vertraglich vereinbarte Datenschutzstandards für internationale Datenübertragungen |
| Betroffenenrechte | Rechte von Personen bezüglich ihrer Daten |
| TLS 1.3 | Transport Layer Security, aktueller Standard für verschlüsselte Datenübertragung |
| AES-256 | Advanced Encryption Standard mit 256-Bit Schlüssellänge für Datenverschlüsselung |
| Salt | Zufällige Daten, die beim Passwort-Hashing zur Erhöhung der Sicherheit verwendet werden |
| Multi-Faktor-Authentifizierung (MFA) | Sicherheitsverfahren mit mehreren Authentifizierungsfaktoren |
| Incident Response | Strukturierter Prozess zur Behandlung von Sicherheitsvorfällen |
| Penetration Testing | Sicherheitstest durch simulierte Angriffe auf IT-Systeme |
| CaaS Provider | Container-as-a-Service Anbieter für Cloud-Infrastruktur |

Tabelle : Glossar 2

Inhaltsverzeichnis

1 Übersicht und Zweck 2

1.1 Management Summary 2

1.2 Zweck dieses Konzeptes 2

2 Rechtliche Grundlagen 2

2.1 Bestehendes Recht 2

2.2 Verantwortlichkeiten 2

2.3 Wichtigkeit 2

3 Datenarten und Zweck 3

3.1 Personenbezogene Daten 3

3.1.1 Stammdaten 3

3.1.2 Nutzungsdaten 3

3.2 Zweck 3

4 Rechtsgrundlagen der Verarbeitung 4

4.1 Art. 6 DSGVO / Art. 13 nDSG 4

4.1.1 Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO): 4

4.1.2 Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO): 4

4.1.3 Einwilligung (Art. 6 Abs. 1 lit. a DSGVO): 4

5 Wiederrufsrecht 5

5.1 Vertragserfüllung 5

5.1.1 Kalenderfunktion 5

5.1.2 Aufgabenverwaltung 5

5.1.3 Benutzerkonto 5

5.2 Nicht Vertragserfüllung fällt: 5

5.2.1 Marketing: 5

5.2.2 Analytics: 5

6 Technische Massnahmen 6

6.1 Wichtigkeit 6

6.2 Verschlüsselung 6

6.3 Zugriffskontrolle 6

6.4 Einstellungen für die Organisation 6

7 Massnahmen 7

7.1 US Server 7

7.2 US Providers 7

7.3 Kalender Integration 7

8 Betroffennenrecht 8

8.1 Auskunftsrecht 8

8.2 Recht auf Berchtigung 8

8.3 Einschränkung auf Verarbeitung 8

8.4 Recht auf Vergessenwerden 8

9 Incident Response 9

9.1 Datenschutzverletzungen 9

9.1.1 Erkennungsmaßnahmen 9

9.1.2 Response-Prozess 9

9.2 Meldeverfahren 9

10 Roadmap 10

10.1 Grundlagen 10

10.2 Erweiterte Massnahmen 10

10.3 Optimierung 10

11 Fazit 11

11.1 Weniger ist mehr 11

11.2 Rechte 11

11.3 Verantwortung 11

11.4 Reaktion 11

11.5 Zeitplan 12

11.5.1 Vor der Veröffentlichung 12

11.6 Zukunft 12

Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis 1

Tabelle 2: Glossar 1 13

Tabelle 3: Glossar 2 14

1. https://www.datenschutz.org/dsgvo-bussgeld/ [↑](#footnote-ref-1)
2. https://haerting.ch/wissen/strafbestimmungen\_des\_neuen\_datenschutzgesetzes/ [↑](#footnote-ref-2)
3. https://www.datenschutzexperte.de/blog/die-rolle-der-dsgvo-beim-unternehmenskauf-due-diligence [↑](#footnote-ref-3)
4. https://www.lfd.niedersachsen.de/startseite/themen/internationaler\_datenverkehr/das\_schrems\_ii\_urteil\_des\_eugh\_und\_seine\_bedeutung\_fur\_datentransfers\_in\_drittlander/das-schrems-ii-urteil-des-europaischen-gerichtshofs-und-seine-bedeutung-fur-datentransfers-in-drittlander-194085.html [↑](#footnote-ref-4)
5. https://www.lfd.niedersachsen.de/startseite/themen/internationaler\_datenverkehr/das\_schrems\_ii\_urteil\_des\_eugh\_und\_seine\_bedeutung\_fur\_datentransfers\_in\_drittlander/das-schrems-ii-urteil-des-europaischen-gerichtshofs-und-seine-bedeutung-fur-datentransfers-in-drittlander-194085.html [↑](#footnote-ref-5)
6. https://blog.idgard.com/de/us-cloud-act-vs-datenschutz/ [↑](#footnote-ref-6)
7. https://www.bfdi.bund.de/DE/Buerger/Basiswissen/Betroffenenrechte/BetroffenenRechte\_node.html [↑](#footnote-ref-7)
8. https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte\_Berichtigung.html [↑](#footnote-ref-8)
9. https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte\_L%C3%B6schung\_Vergessenwerden.html [↑](#footnote-ref-9)