

## 4.7 privacy & data lifecycle

حریم خصوصی و چرخه حیات داده - ProDecks

نسخه: 1.0

تاریخ: 1403/11/16

اصول GDPR منطبق با - MVP: وضعیت

### ProDecks فصل ۱: فلسفه حریم خصوصی در

#### ۱.۱. تعهد ما

است. ما متعهد به جمع‌آوری، پردازش و نگهداری داده‌ها ProDecks احترام به حریم خصوصی کاربران اولویت اصلی "به شیوه‌ای شفاف، امن و مطابق با قوانین هستیم"

#### ۱.۲. اصول حریم خصوصی

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

#### ۱.۳. حوزه اجرایی

- ProDecks کلیه داده‌های کاربران
- تمام مناطق جغرافیایی
- همه انواع داده‌ها (شخصی، پروژه‌ای، رفتاری)

### فصل ۲: طبقه‌بندی داده‌ها

#### ۲.۱. داده‌های شخصی

- اطلاعات هویتی: نام، ایمیل، شماره تلفن
- (شده hash) اطلاعات حساب: نام کاربری، رمز عبور
- اطلاعات پروفایل: عکس، بیوگرافی
- اطلاعات دستگاه، IP، اطلاعات ارتباطی: آدرس

#### ۲.۲. داده‌های پروژه‌ای

- نام، توضیحات، اعضا: Spaces
- نام، رنگ، موقعیت: Decks
- عنوان، توضیحات، مسئول، تاریخ‌ها: Cards
- اطلاعات کارت‌های زیرمجموعه: Subcards

## داده‌های رفتاری ۲.۳.

- فعالیت‌های کاربر: ورود، ایجاد کارت، تکمیل کارت
- تعاملات: دعوت اعضا، کامنت‌ها
- ترجیحات: تنظیمات کاربری
- استفاده patterns، تحلیل: زمان صرف شده

## داده‌های حساس ۲.۴.

- در حال حاضر: هیچ داده حساسی جمع‌آوری نمی‌شود
- PCI DSS با رعایت (در آینده: اطلاعات پرداخت)

---

## فصل ۳: چرخه حیات داده

---

Collection → Processing → Storage → Sharing → Archival → Deletion

### (Collection) مرحله ۱: جمع‌آوری ۳.۱.

روش‌های جمع‌آوری:

ثبت‌نام مستقیم کاربر ۱.

فعالیت‌های کاربر در پلتفرم ۲.

سیستم‌های تحلیلی ۳.

(Consent) رضایت:

رضایت صریح برای داده‌های شخصی -

از جمع‌آوری داده‌های تحلیلی opt-out امکان -

شفافیت در اهداف جمع‌آوری -

### (Processing) مرحله ۲: پردازش ۳.۲.

اهداف پردازش:

ارائه خدمات اصلی ۱.

بهبود محصول ۲.

compliance امنیت و ۳.

ارتباط با کاربران ۴.

محدودیت‌های پردازش:

فقط برای اهداف تعیین شده -

حداقل داده لازم -







- AES-256: در حال ذخیره -

- bcrypt: رمز عبور -

- Access Control:
  - Role-Based Access Control
  - Least Privilege Principle
- Multi-factor Authentication (آینده)

- Network Security:
  - فایروال
  - IDS/IPS
  - DDoS protection

## ۶.۲. کنترل‌های اداری

- آموزش حریم خصوصی برای کارکنان
- قراردادهای محرمانگی
- دسترسی مبتنی بر نیاز

## ۶.۳. کنترل‌های فیزیکی

- میزبانی در دیتاسنترهای امن
- کنترل دسترسی فیزیکی
- امن رسانه‌ها destruction

---

## فصل ۷: اشتراک‌گذاری داده با شخص ثالث

---

### ۷.۱. ارائه‌دهندگان خدمات

#### ۱. میزبانی (Hosting Provider)

- داده‌های منتقل‌شده: تمام داده‌های کاربر
- هدف: ارائه خدمات میزبانی
- قرارداد: شامل بندهای حفاظت از داده

#### ۲. خدمات تحلیلی (Analytics)

- داده‌های منتقل‌شده: داده‌های ناشناس‌شده
- هدف: تحلیل استفاده از محصول
- قبل از ارسال anonymization: روش

#### ۳. خدمات ایمیل (Email Service)

- داده‌های منتقل‌شده: ایمیل کاربران
- هدف: ارسال اعلان‌ها
- قرارداد: عدم استفاده برای اهداف دیگر

### ۷.۲. الزامات قراردادی









- درخواست دسترسی به داده
- درخواست حذف حساب
- مدیریت رضایت‌ها

## ابزارهای مدیریتی ۱۳.۲

- مدیریت حریم خصوصی dashboard
- anonymization ابزارهای
  - auditing سیستم
  - reporting ابزارهای

## ابزارهای فنی ۱۳.۳

- encryption tools
- access control systems
- logging و monitoring tools

---

## فصل ۱۴: چالش‌ها و راه‌حل‌ها

---

### چالش: تعادل بین کارایی و حریم خصوصی ۱۴.۱

- داده‌های تحلیلی anonymization: راه‌حل
- (Differential Privacy) راه‌حل: به‌کارگیری تفاضل حریم خصوصی

### چالش: همکاری تیمی و حریم خصوصی ۱۴.۲

- دسترسی granular راه‌حل: تنظیمات
- راه‌حل: آموزش کاربران

### چالش: مقررات چندگانه ۱۴.۳

- راه‌حل: تطبیق با سخت‌ترین استاندارد
- راه‌حل: مشاوره حقوقی تخصصی

---

## فصل ۱۵: نقشه راه حریم خصوصی

---

### (MVP - فعلی) فاز ۱ ۱۵.۱

- پیاده‌سازی اصول اولیه حریم خصوصی
- کامل Privacy Policy
- ابزارهای اولیه مدیریت حریم خصوصی

### فاز ۲ (۶ ماهه) ۱۵.۲

- GDPR پیاده‌سازی کامل حقوق کاربران

