سند ۴,۷: حریم خصوصی و چرخه عمر داده (مطابق با GDPR) — ShahnamehMap

نسخه: ۱,۰

تاریخ: ۲۵/۰۸/۱۴۰۳

تهیه‌کننده: مدیرعامل (CEO) با مشاوره حقوقی

وضعیت: محرمانه

بازبینی: سالانه یا با تغییر عمده در پردازش داده

---

۱۰. مقدمه و اصول حاکم (Governance Principles)

این سند چارچوب مدیریت داده‌های شخصی در ShahnamehMap را بر اساس اصول حریم خصوصی از طراحی (Privacy by Design & Default) و GDPR و آمادگی برای استانداردهای جهانی مانند قانون حمایت از داده‌های ایران تعریف می‌کند. هدف، ایجاد اعتماد و پایبندی به اخلاق دیجیتال است.

:اصول کلیدی

۱. **قانونمندی، انصاف و شفافیت:** داده تنها با رضایت آگاهانه و برای اهداف مشخص جمع‌آوری می‌شود.

۲. **محدودیت هدف:** داده فقط برای اهداف تعریف‌شده در زمان جمع‌آوری استفاده می‌شود.

۳. **حداقل داده:** تنها داده‌های ضروری برای تحقق هدف جمع‌آوری می‌شوند.

۴. **دقت:** داده‌ها دقیق و به‌روز نگه داشته می‌شوند.

۵. **محدودیت ذخیره‌سازی:** داده‌ها فقط برای مدت لازم حفظ می‌شوند.

۶. **امنیت و محرمانگی:** یکپارچگی و محرمانگی داده از طریق کنترل‌های فنی و سازمانی تضمین می‌شود.

۷. **پاسخگویی:** ما مسئول رعایت این اصول و نمایش آن هستیم.

---

۲. **نقش‌ها و مسئولیت‌ها (Roles & Responsibilities)**

نهاد در** | **GDPR نقش** | **تعریف طبق** |
| **مسئولیت کلیدی** | **ShahnamehMap

| :--- | :--- | :--- | :--- |

نهادی که اهداف و ابزارهای پردازش داده | **Data Controller** |
مالک) شخصی را تعیین می‌کند. | **شرکت الفبا شید
کسب •
.تعیین هدف پردازش • | **(ShahnamehMap
| data subject. پاسخ به درخواست‌های •
.رضایت

نهادی که داده را به نمایندگی از | **Data Processor** |
پردازش می‌کند. | • ارائه‌دهنده میزبانی کلاد (مثلاً Controller
Google Analytics**) سرویس آنالیتیکس •
دیجی‌کالا کلاد)
سرویس پرداخت •
(**SendGrid**) سرویس ایمیل •
(**4
•
.Controller پردازش داده مطابق دستورات • |(**ZarinPal**)
| .گزارش نقض داده •
.اجرای اقدامات امنیتی

ناظر مستقل بر انطباق. | | **Data Protection Officer (DPO)** |
این وظایف را بر عهده دارد. با **(CEO) در حال حاضر، **مدیرعامل
مستقل DPO رسیدن به مقیاس (۱۰۰،۰۰۰ کاربر در اتحادیه اروپا)، یک
نقطه تماس برای مراجع •
.منصوب خواهد شد. | • نظارت بر انطباق
| .آموزش کارکنان •
.نظارتی و کاربران

Data Processing قرارداد **:(DPAs) توافق‌نامه‌های الزام‌آور
منعقد **Processors** استاندارد با **همه **Addendum (DPA)**
به رعایت اصول Processor ها متضمن تعهدDPA شده یا خواهد شد. این
.و همکاری در زمینه امنیت و پاسخ به درخواست‌ها هستند GDPR

---

۳. فهرست پردازش داده (Records of Processing Activities - RoPA)

.این جدول اصلی، چرخه عمر هر دسته داده را مستند می‌کند

| دسته داده** | **هدف پردازش (قانونی)** | **جمع‌آوری** | ** |
| Third **ذخیره‌سازی** | **دسترسی داخلی** | **اشتراک‌گذاری با
| **مدت نگهداری** | **روش حذف/ناشناس‌سازی** | **Party**
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| اطلاعات حساب کاربری** (ایمیل، هش رمز عبور، نام نمایشی) | انجام ** |
| .قرارداد (ارائه سرویس)، رضایت. | فرم ثبت‌نام در سایت
در کلاد ایران (رمزنگاری شده در حالت استراحت). | **PostgreSQL**

SendGrid | .تیم فنی (برای پشتیبانی)، سیستم‌های احراز هویت برای ایمیل‌های تراکنش). | تا **۲۴ ماه** پس از آخرین ورود کاربر. پس از آن، **حذف خودکار** یا **ناشناس‌سازی**. | روند حذف از بخش ۴ | .

پروفایل بازیکن/کاراکتر** (نژاد، کلاس، امتیازات، تاریخچه بازی) | ** | انجام قرارداد (اجرای بازی)، علایق مشروع (بهبود بازی). | فرم ساخت کاراکتر (state) **Redis**، (کاراکترها) **PostgreSQL** | .و لاگ بازی تیم فنی، تیم محصول (برای تحلیل تعادل بازی). | | .(جلسه فعال **خیر**. | تا **۱۲ ماه** پس از غیرفعال شدن حساب کاربری. | همراه با حساب کاربری. |

متن کمپین‌های ساخته‌شده) |) **(UGC) داده‌های محتوای کاربر** | Campaign Builder. | ابزار | .(ToS در) رضایت صریح کاربر تصاویر آپلودشده). | تیم محتوا) **MinIO**، (ساختار) **Neo4j** (برای بررسی انطباق). | **خیر** (جز در صورت انتشار عمومی توسط کاربر). | تا زمانی که کاربر آن را **حذف کند** + **۶ ماه** بایگانی (برای حل اختلاف). | حذف از دیتابیس‌ها و storage. |

داده‌های تراکنش مالی** (شناسه پرداخت، مبلغ، تاریخ) | تعهد قانونی ** | رمزنگاری) **PostgreSQL** | .(مالیاتی). | درگاه پرداخت زرین‌پال پردازشگر پرداخت)،) **ZarinPal** | .شده). | مدیر مالی، حسابرس

حسابرس قانونی. | **۱۰ سال** مطابق قانون مالیات. | پس از ۱۰ سال، | .**حذف امن**

| (هاEventکلیک‌ها، مسیرهای بازی،) **داده‌های تحلیلی رفتاری** | GA4) علایق مشروع (تحلیل و بهبود محصول). | کدهای ردیابی در فرانت‌اند در کلاد ایران). | تیم محصول، تحلیلگر) **ClickHouse** | .(داخلی تنها در صورت فعال‌کردن کاربر). |) **Google Analytics 4** | .داده سپس **حذف خودکار**. | .(GA4 تنظیم پیش‌فرض در) **۱۴** ماه | .ها پس از ۲۴ ساعت ناشناس می‌شوندClickHouse. IP حذف دوره‌ای از

نام مدرسه، نام معلم، تعداد دانش‌آموزان) |) **(B2B) داده‌های مدرسه** | | .انجام قرارداد با مدرسه. | فرم درخواست مدرسه و مذاکره
، پشتیبانی. | B2B جدول جداگانه). | مدیر فروش) **PostgreSQL** | .**خیر**. | **۵ سال** پس از اتمام قرارداد. | حذف امن

(Data Subject Rights) چرخه حیات داده و حقوق اشخاص .۴ ##

(Collection & Consent) جمع‌آوری و رضایت .۴,۱ ###

* **شفافیت:** خط‌مشی حریم خصوصی (Privacy Policy)** به زبان ساده در صفحه ثبت‌نام لینک شده است.

* **رضایت صریح:** برای پردازش‌های خاص (مانند دریافت خبرنامه یا مارکتینگ)، چک‌باکس **opt-in** جداگانه استفاده می‌شود.

* **حق انصراف:** کاربر می‌تواند در هر زمان از طریق تنظیمات پروفایل، رضایت خود را لغو کند.

۴,۲. ذخیره‌سازی و پردازش (Storage & Processing)**

* **محل ذخیره‌سازی:** تمامی داده‌های کاربران ایرانی در سرورهای داخل ایران ذخیره می‌شود، مگر در موارد استثنا (مثلاً برخی سرویس‌های تحلیل که رضایت گرفته شده است).

* **امنیت:** مطابق سند ۴,۶ (امنیت).

۴,۳. حذف و ناشناس‌سازی (Deletion & Anonymization)**

* **درخواست حذف (Right to Erasure / "حق فراموشی"):** کاربر می‌تواند از طریق صفحه "حریم خصوصی من" در پنل کاربری یا ارسال ایمیل به `privacy@shahnamehmap.ir` درخواست حذف کامل دهد.

* **روند حذف کامل حساب:**

.تأیید هویت** کاربر از طریق لینک ایمیل** ۱.

.لغو تمام اشتراک‌های فعال** و قطع دسترسی** ۲.

نشانه‌گذاری حساب** به عنوان "در حال حذف" و شروع دوره ** ۳.
.برای جلوگیری از حذف تصادفی **(Grace Period) **۳۰ روزه تعلیق

:پس از ۳۰ روز، اجرای **اسکریپت حذف امن** که ۴.

* **PostgreSQL** ایمیل و شناسه‌های شخصی را از دیتابیس
.پاک می‌کند

* برای تحلیل‌های جمعی **ClickHouse** داده‌های کاربر را در
می‌کند (تبدیل به داده‌های تجمیعی **(Anonymize) **ناشناس
.غیرقابل انتساب)

* .حذف می‌کند **MinIO** فایل‌های آپلودشده کاربر را از

۵. کاربر پس از **۹۰ روز** به طور IP لاگ‌های سرور** حاوی**
.خودکار حذف می‌شوند

* استثناها:** داده‌های مالی طبق قانون، و داده‌های مربوط به حل ** *
اختلاف یا ادعای قانونی ممکن است برای مدت طولانی‌تری (با محدودیت
.دسترسی) نگهداری شوند

۴,۴. حقوق دیگر اشخاص (Other Data Subject Rights)

:ما مکانیسمی ساده در پنل کاربری برای اعمال این حقوق ایجاد کرده‌ایم

* **حق دسترسی (Right of Access):** کاربر می‌تواند **خروجی JSON کامل از داده‌های شخصی خود در قالب (Export)** دریافت کند.

* **حق تصحیح (Right to Rectification):** کاربر می‌تواند اطلاعات پروفایل خود را مستقیم ویرایش کند.

* **حق محدود کردن پردازش (Right to Restrict Processing):** کاربر می‌تواند حساب خود را "معلق" کند.

* **حق انتقال‌پذیری داده (Right to Data Portability):** خروجی JSON فوق، قابلیت انتقال به سرویس دیگر را فراهم می‌کند.

* **حق اعتراض (Right to Object):** کاربر می‌تواند به پردازش برای اهداف بازاریابی مستقیم اعتراض کند (و بلافاصله متوقف می‌شود).

---

۵. **مدیریت داده در سطح طراحی (Privacy by Design)**

* **Data Minimization** در فرم‌ها: از کاربران اطلاعات غیرضروری (مانند جنسیت، تاریخ تولد) پرسیده نمی‌شود.

* **Pseudonymization:** در سیستم تحلیل (**ClickHouse**)، شناسه کاربر با یک شناسه ناشناس (UUID) جایگزین می‌شود تا تحلیل‌گران مستقیم به ایمیل دسترسی نداشته باشند.

* **کنترل‌های دسترسی دقیق:** حتی توسعه‌دهندگان داخلی نیز به **production** دسترسی ندارند. دسترسی بر طور پیش‌فرض به دیتابیس‌ها **رد** است و با **نیاز-به-دانستن** (Need-to-Know) اساس نقش (Role-Based) اعطا می‌شود.

---

۶. آموزش و پاسخ به رویداد (Training & Incident Response)

* **آموزش کارکنان:** همه کارکنان فنی و غیرفنی در بدو استخدام، و **حریم خصوصی** را می‌آموزند و سالانه بازآموزی می‌بینند.

* **پروتکل پاسخ به حادثه (Data Breach):** سند **۴,۶** شامل بخش **اطلاع‌رسانی به مراجع نظارتی و کاربران آسیب‌دیده**، اطلاع‌رسانی به مرجع GDPR در صورت وقوع نقض داده شخصی است. طبق نظارتی باید حداکثر ظرف **۷۲ ساعت** انجام شود.

---

۷. ارزیابی تاثیر حریم خصوصی (Privacy Impact Assessment - PIA)

* **چه زمانی:** قبل از راه‌اندازی **هر ویژگی جدید یا تغییر اساسی** که پردازش داده را به طور قابل توجهی تغییر دهد (مثلاً افزودن سیستم چت صوتی، ادغام با یک شبکه اجتماعی).
* **چه چیزی:** ارزیابی می‌کند که آیا پردازش جدید با اصول حریم خصوصی سازگار است، ریسک‌های جدیدی ایجاد می‌کند و آیا کنترل‌های کافی دارد.
* **نتیجه:** ممکن است منجر به **تغییر طراحی، افزودن کنترل‌های جدید، یا مشاوره با DPO/مشاور حقوقی** شود.

---

۸. نتیجه: آینده‌نگری به جای واکنش به بحران

حریم خصوصی را نه به ShahnamehMap این سند نشان می‌دهد که عنوان یک **مزاحم قانونی برای آینده**، بلکه به عنوان یک **قابلیت اساسی و مزیت رقابتی** از روز اول در نظر گرفته است. با مستندسازی چرخه عمر داده، تعریف نقش‌ها، و طراحی فرآیندهای حذف و پاسخ به درخواست‌ها، ما:

۱. **اعتماد کاربران را جلب می‌کنیم:** کاربران می‌دانند بر داده خود کنترل دارند.

۲. **از جریمه‌های سنگین آینده جلوگیری می‌کنیم:** رویکرد پیش‌دستانه، هزینه انطباق را به شدت کاهش می‌دهد.

۳. **عملکرد تیم را بهبود می‌بخشیم:** داشتن نقشه واضح از داده، تصمیم‌گیری محصول و معماری فنی را آسان‌تر می‌کند.

۴. **بستر را برای گسترش بین‌المللی آماده می‌کنیم:** پایبندی به GDPR.، ورود به بازار اروپا و دیاسپورا را ممکن می‌سازد

حریم خصوصی یک ویژگی نیست، یک زیرساخت است.** سرمایه‌گذاری **
روی این زیرساخت اکنون، از بحران‌های حقوقی، مالی و اعتباری پرهزینه در
.آینده جلوگیری خواهد کرد