Privacy & Data Lifecycle (GDPR-ready)

۴٫۷٫۱ مقدمه و پایه قانونی

سیستم نوبت‌دهی `nobatnou.ir` داده‌های شخصی کاربران را جمع‌آوری و پردازش می‌کند. این سند بر اساس اصول **مقررات عمومی حفاظت از داده‌ها (GDPR)** و قوانین حریم خصوصی ایران، چرخه حیات داده‌ها، نقش‌های مسئول، و اقدامات حفاظتی را تشریح می‌کند. هدف، شفاف‌سازی و تضمین حقوق داده‌های اشخاص (Data Subjects) است.

۴٫۷٫۲ نقش‌ها (Roles) بر اساس GDPR**

نقش	مسئولیت	موجود در سیستم
Controller (کنترل‌کننده)	تعیین اهداف و روش‌های پردازش داده	شرکت «نوبت نو» (صاحب `nobatnou.ir`)
Processor (پردازشگر)	پردازش داده‌ها به دستور کنترل‌کننده	میزبانی وب (هاست)، سرویس‌های ابری (اگر استفاده شود)
Data Subject (صاحب داده)	فردی که داده‌هایش پردازش می‌شود	کاربران ثبت‌نام‌شده یا نوبت‌گیرندگان

توافقنامه پردازش داده (Data Processing Agreement - DPA):

- بین کنترل‌کننده (نوبت نو) و پردازشگر (هاست) منعقد شده است.

- شامل بندهای محرمانگی، امنیت داده، و همکاری در صورت درخواست مقام نظارتی می‌شود.

۴٫۷٫۳ **داده‌های شخصی جمع‌آوری‌شده**

دسته داده	عناصر داده	پایه قانونی پردازش	حساسیت
اجرای قرارداد	بالا	نام کامل، شماره تلفن	رضایت صریح (Consent) + اجرای قرارداد	بالا
داده‌های نوبت‌دهی	زمان نوبت، موقعیت در صف، وضعیت، پزشک مورد نظر	اجرای قرارداد (ارائه سرویس)	متوسط
داده‌های احراز هویت	رمز عبور (هش‌شده)	اجرای قرارداد	بالا
داده‌های فنی	IP، user agent، timestamp	منافع مشروعیت (Legitimate Interests)	پایین

منبع داده:

- مستقیم از کاربران از طریق فرم‌های وب‌سایت.

.جمع‌آوری نمی‌شود (Third Parties) هیچ داده‌ای از منابع ثالث -

---

۴٫۷٫۴ چرخه حیات داده (Data Lifecycle)

مرحله ۱: جمع‌آوری (Collection)**

- روش:** فرم‌های HTML با فیلدهای الزامی.
- رضایت (Consent):**
- و دریافت تأیید کاربر (چک‌باکس) در زمان ثبت‌نام **سیاست حریم خصوصی** نمایش.
- ارائه امکان عدم موافقت (با این حال دسترسی به سرویس محدود می‌شود).
- شفافیت:** اعلام هدف جمع‌آوری (ارائه نوبت، پیگیری وضعیت) در محل جمع‌آوری**.

مرحله ۲: ذخیره‌سازی (Storage)**

- محل ذخیره‌سازی:**
- پایگاه‌داده MySQL (ایران) روی سرور میزبانی داخلی.
- جداول: `wp_nobat_users`، `wp_nobat_system`.
- مدت نگهداری (Retention Period):**

نوع داده	مدت نگهداری	دلیل

| داده‌های نوبت‌های تکمیل‌شده | ۲۴ ماه | پاسخ به شکایات، تحلیل عملکرد |

| داده‌های نوبت‌های لغوشده | ۱۲ ماه | اسناد حسابداری احتمالی |

| حساب‌های کاربری غیرفعال | ۱۸ ماه پس از آخرین ورود | بازیابی حساب توسط کاربر |

| لاگ‌های دسترسی (access logs) | ۶ ماه | امنیت و عیب‌یابی |

رمزنگاری در حالت ذخیره: -

- رمز عبور با الگوریتم bcrypt هش می‌شود.

- شماره تلفن در حال حاضر رمزنگاری نشده (نیاز به پیاده‌سازی دارد).

مرحله ۳: پردازش (Processing)**

پردازش‌های انجام‌شده: -

- مرتب‌سازی نوبت‌ها بر اساس موقعیت (position).

- محاسبه زمان تخمینی ویزیت.

- ارسال یادآوری (در صورت پیاده‌سازی در آینده).

اشتراک‌گذاری داده (Data Sharing): -

- داده‌ها با **هیچ شخص ثالثی** به اشتراک گذاشته نمی‌شود.

- تنها در صورت درخواست مقام قضایی، داده‌ها افشا می‌شوند.

مرحله ۴: به‌روزرسانی (Updating)**

- کاربران می‌توانند از طریق **داشبورد کاربری** نام خود را به‌روز کنند.

- شماره تلفن قابل تغییر نیست (نیاز به ایجاد حساب جدید است).

مرحله ۵: حذف** (Deletion) / فراموشی (Right to be Forgotten)**

روش‌های حذف داده:

۱. **حذف خودکار:** پس از پایان مدت نگهداری، داده‌ها به‌طور خودکار از دیتابیس (با cron job) حذف می‌شوند.

۲. **حذف دستی:** کاربر می‌تواند درخواست حذف حساب خود را از طریق تماس با پشتیبانی ارائه دهد.

فرآیند درخواست حذف:

- کاربر درخواست خود را به آدرس `privacy@nobatnou.ir` ارسال می‌کند.
- تیم پشتیبانی هویت کاربر را تأیید می‌کند (از طریق تماس تلفنی).
- حذف داده‌های کاربر از همه جداول (`nobat_users`, `nobat_system`) می‌شود.
- تأیید حذف به کاربر اطلاع داده می‌شود.

استثناها: داده‌های مالی (در صورت وجود) ممکن است برای رعایت قوانین مالیاتی تا ۷ سال نگهداری شوند.

۴٫۷٫۵ دسترسی به داده (Access Control)

افراد دارای دسترسی

| نقش | دسترسی به داده | دلیل دسترسی | محدودیت‌ها |

| ------ | ---------- | ---------- | ---------- |

| توسعه‌دهنده اصلی** | دسترسی کامل به دیتابیس | عیب‌یابی، بهینه‌سازی | دسترسی ** |
VPN + 2FA از طریق |

| پاسخ به مشکلات کاربران | (read-only) پشتیبانی فنی** | دسترسی فقط‌خوانی** |
ثابت، لاگ‌گیری کامل IP |

| مدیر سیستم** | دسترسی به لاگ‌های سرور | امنیت و نظارت | دسترسی محدود به ** |
دایرکتوری‌های خاص |

کنترل‌های دسترسی:

- احراز هویت قوی برای پنل مدیریت وردپرس.

- جداسازی محیط تست از محیط تولید (تست با داده‌های ساختگی).

- بررسی دسترسی‌ها هر ۶ ماه یکبار.

۴٫۷٫۶ حقوق صاحبان داده (Data Subject Rights)

سیستم حق‌های زیر را برای کاربران فراهم می‌کند:

حق	نحوه اجرا در سیستم
۱. حق دسترسی (Right of Access)	کاربران می‌توانند همه داده‌های خود را در **داشبورد کاربری** مشاهده کنند.
۲. حق تصحیح (Right to Rectification)	ویرایش نام از طریق داشبورد (شماره تلفن غیرقابل تغییر است).
۳. حق حذف (Right to Erasure)	درخواست از طریق ایمیل به `privacy@nobatnou.ir`.
۴. حق محدود کردن پردازش (Right to Restriction)	کاربر می‌تواند حساب خود را به حالت «تعلیق» ببرد (موقتاً غیرفعال شود).
۵. حق اعتراض (Right to Object)	عدم دریافت هرگونه پیام تبلیغاتی (در صورت راه‌اندازی).
۶. حق انتقال داده (Right to Data Portability)	امکان دریافت داده‌های خود در قالب JSON از طریق درخواست به پشتیبانی.

مکانیسم اجرای حقوق:

- صفحه **«حریم خصوصی و حقوق شما»** در وب‌سایت با توضیح کامل حقوق.
- فرم درخواست آنلاین برای اعمال حقوق (در حال توسعه).

- **پاسخ به درخواست‌ها حداکثر ظرف ۳۰** روز.

۴/۷/۷ امنیت و حفاظت از داده

اقدامات فنی** (Technical Measures)**

- **رمزنگاری در انتقال:** TLS 1.3 برای همه صفحات.
- **رمزنگاری در ذخیره:** هش رمز عبور با bcrypt.
- **کنترل دسترسی:** احراز هویت دو مرحله‌ای برای ادمین‌ها.
- **پشتیبان‌گیری:** backup روزانه با encryption و نگهداری در مکان جداگانه.
- **حفاظت در برابر نفوذ:** WAFها، به‌روزرسانی منظم وردپرس و پلاگین‌ها.

اقدامات سازمانی** (Organizational Measures)**

- **آموزش کارکنان:** دوره‌های آشنایی با GDPR و حریم خصوصی.
- **تکمیل موافقت‌نامه محرمانگی** (NDA)** برای همه کارکنان و پیمانکاران.
- **ممیزی داخلی هر ۱۲ ماه:** بررسی دوره‌ای.

۴/۷/۸ **انتقال داده به خارج از کشور**

- **سیاست فعلی:** تمام داده‌ها در سرورهای داخل ایران نگهداری می‌شوند.
- **در صورت انتقال آینده:** رعایت فصل ۵ GDPR (شرکت قواعد، کافی حفاظت‌های الزام‌آور).
- **ثبت انتقال:** در سوابق پردازش فعالیت‌ها (Records of Processing Activities - ROPA) ثبت خواهد شد.

۴/۷/۹ **واکنش به نقض حریم خصوصی (Data Breach Response)**

فرآیند اطلاع‌رسانی:

۱. **شناسایی نقض** (ظرف ۲۴ ساعت).

۲. **ارزیابی ریسک** (آیا خطر برای حقوق افراد وجود دارد؟).

۳. **در صورت ریسک بالا:** اطلاع‌رسانی به **مرجع نظارتی** ظرف ۷۲ ساعت.

۴. **در صورت ریسک بسیار بالا:** اطلاع‌رسانی به **افراد affected** بدون تأخیر.

اطلاعات قابل افشا در صورت نقض:

- ماهیت نقض.
- داده‌های درگیر.

.اقدامات انجام‌شده برای کاهش آسیب -

.راه‌های تماس برای دریافت اطلاعات بیشتر -

۴٫۷٫۱۰** سوابق پردازش فعالیت‌ها (Records of Processing Activities - ROPA)**

| بخش | توضیح |

| --- | --- |

| هدف پردازش** | ارائه سرویس نوبت‌دهی پزشکی** |

| انواع داده** | نام، شماره تلفن، زمان نوبت** |

| ذینفعان** | کاربران نهایی (بیماران)** |

| گیرندگان داده** | هیچ شخص ثالثی** |

| مدت نگهداری** | مطابق جدول بخش ۴٫۷٫۴** |

| اقدامات امنیتی** | رمزنگاری، کنترل دسترسی، ** WAF |

۴/۷/۱۱ ارزیابی تأثیر حریم خصوصی (Privacy Impact Assessment - PIA)

پروژه‌های نیازمند PIA (در صورت اجرا):

- افزودن سیستم پیامک یادآوری نوبت.
- یکپارچه‌سازی با سامانه‌های بیمارستانی (EMR).
- استفاده از تحلیل‌گر رفتار کاربر (Analytics) پیشرفته.

ساختار PIA:

۱. توصیف پردازش.

۲. ارزیابی ضرورت و تناسب.

۳. شناسایی ریسک‌های حریم خصوصی.

۴. اقدامات کاهش ریسک.

۵. تأییدیه مدیریت.

۴/۷/۱۲ مستندات و سیاست‌های مرتبط

| سند | هدف | دسترسی |

| ------ | ------ | --------- |

| اطلاع‌رسانی به کاربران | **(Privacy Policy) سیاست حریم خصوصی** | لینک در فوتر سایت |

| رابطه با پردازشگرها | داخلی (محرمانه) | **(DPA) موافقت‌نامه پردازش داده** |

| راهنمای پاسخ به نقض داده** | واکنش به حوادث | داخلی** |

| منشور اخلاق داده** | راهنمای کارکنان | داخلی** |

نتیجه‌گیری ۴۰۷۰۱۳

از مرحله طراحی، حریم خصوصی و اصول `nobatnou.ir` این سند نشان می‌دهد که GDPR را در نظر گرفته است. با پیاده‌سازی چرخه حیات داده کنترل‌شده، تعریف نقش‌های شفاف، و تضمین حقوق کاربران، پایه‌ای محکم برای توسعه آینده با کم‌ترین ریسک قانونی فراهم شده است. بازبینی دوره‌ی این سند و تطبیق با قوانین جدید الزامی است.