Privacy & Data Lifecycle (GDPR-Ready)

مقدمه و هدف سند

این سند با هدف تشریح کامل چرخه عمر داده‌ها در پروژه Metrogo تدوین شده است Metrogo . به‌عنوان یک محصول فناورانه در حوزه حمل‌ونقل شهری و مترو، به‌صورت ذاتی با داده‌هایی سروکار دارد که مستقیماً به رفتار، هویت، الگوهای تردد و در برخی موارد اطلاعات مالی کاربران مرتبط هستند. از همین رو، مدیریت صحیح داده‌ها نه‌تنها یک الزام فنی، بلکه یک ضرورت حقوقی، تجاری و اعتباری محسوب می‌شود.

این سند تلاش می‌کند نشان دهد که تیم Metrogo از مراحل اولیه توسعه، نگاه آینده‌نگر به موضوع حریم خصوصی داشته و داده را صرفاً به‌عنوان یک منبع برای توسعه محصول نمی‌بیند، بلکه آن را دارایی‌ای می‌داند که سوءمدیریت آن می‌تواند منجر به جریمه‌های قانونی، از دست رفتن اعتماد کاربران، آسیب به برند و حتی توقف فعالیت کسب‌وکار شود.

نگاه کلان Metrogo به داده و حریم خصوصی

در Metrogo اصل بنیادین این است که حداقل داده لازم برای ارائه ارزش جمع‌آوری شود. این رویکرد برخلاف بسیاری از محصولات اولیه است که داده را «برای آینده» انباشته می‌کنند بدون آنکه هدف مشخصی داشته باشند. درMetrogo ، هر داده‌ای که وارد سیستم می‌شود باید پاسخ روشنی به این سؤال داشته باشد:

»این داده دقیقاً چه ارزشی برای کاربر یا سیستم ایجاد می‌کند؟«

در صورتی که پاسخی برای این سؤال وجود نداشته باشد، داده اساساً جمع‌آوری نمی‌شود. این رویکرد باعث کاهش ریسک، ساده‌سازی معماری داده و افزایش اعتماد کاربران می‌شود.

منشأ داده‌ها در Metrogo

داده‌ها در Metrogo از چند مسیر مشخص وارد سیستم می‌شوند. مهم‌ترین منبع داده، تعامل مستقیم کاربران با اپلیکیشن Metrogo است. کاربران هنگام ثبت‌نام، استفاده از خدمات، انجام پرداخت‌ها یا مشاهده مسیرها، اطلاعاتی را به‌صورت آگاهانه یا ناخواسته در اختیار سیستم قرار می‌دهند. این داده‌ها شامل اطلاعات هویتی، داده‌های رفتاری، داده‌های مکانی و داده‌های تراکنشی هستند.

علاوه بر کاربران، برخی داده‌ها از طریق سرویس‌های شخص ثالث وارد سیستم می‌شوند؛ مانند درگاه‌های پرداخت، سرویس‌های اطلاع‌رسانی شهری یا زیرساخت‌های مرتبط با مترو. این داده‌ها معمولاً به‌صورت محدود و تحت قراردادهای مشخص وارد سیستم می‌شوند و Metrogo اختیار استفاده آزادانه از آن‌ها را ندارد.

در نهایت، بخشی از داده‌ها به‌صورت سیستمی و داخلی تولید می‌شوند؛ مانند لاگ‌ها، داده‌های مانیتورینگ، داده‌های خطا و گزارش‌های عملکرد که برای تضمین پایداری و امنیت سیستم ضروری هستند.

تفکیک و طبقه‌بندی داده‌ها

یکی از نقاط ضعف بسیاری از پروژه‌های نوپا، نداشتن طبقه‌بندی شفاف داده‌هاست. در Metrogo داده‌ها از ابتدا به‌صورت ساختاریافته طبقه‌بندی شده‌اند. این طبقه‌بندی نه‌تنها از منظر فنی، بلکه از منظر حقوقی و مدیریتی نیز اهمیت دارد.

داده‌های هویتی شامل اطلاعاتی هستند که امکان شناسایی مستقیم یا غیرمستقیم کاربر را فراهم می‌کنند. این داده‌ها بالاترین سطح حساسیت را دارند و دسترسی به آن‌ها به‌شدت محدود شده است. داده‌های تراکنشی نیز اگرچه مستقیماً هویت فرد را نشان نمی‌دهند، اما به دلیل ارتباط با امور مالی، در سطح حساسیت بالا قرار می‌گیرند.

داده‌های رفتاری و تحلیلی، اگر به‌صورت خام نگهداری شوند، می‌توانند منجر به بازشناسایی کاربران شوند. به همین دلیل در Metrogo این داده‌ها پس از جمع‌آوری، وارد فرآیند ناشناس‌سازی می‌شوند. داده‌های فنی و سیستمی نیز اگرچه معمولاً حاوی اطلاعات شخصی نیستند، اما در صورت افشا می‌توانند زیرساخت را در معرض حمله قرار دهند، بنابراین مدیریت آن‌ها نیز اهمیت بالایی دارد.

مسیر جریان داده(Data Flow)

در Metrogo مسیر حرکت داده از لحظه ورود تا حذف نهایی آن کاملاً مشخص است. داده ابتدا در لایه جمع‌آوری وارد می‌شود، سپس در لایه پردازش مورد استفاده قرار می‌گیرد و در نهایت در لایه ذخیره‌سازی نگهداری یا حذف می‌شود. هر لایه دارای کنترل‌های امنیتی، محدودیت دسترسی و سیاست‌های مشخص است.

این شفافیت باعث می‌شود در هر لحظه بتوان پاسخ داد که «این داده اکنون کجاست، چه کسی به آن دسترسی دارد و تا چه زمانی باقی می‌ماند.«

ذخیره‌سازی داده و معماری انتخاب‌شده

Metrogoاز زیرساخت ابری با استانداردهای امنیتی بالا استفاده می‌کند. داده‌های حساس در دیتابیس‌های رمزنگاری‌شده ذخیره می‌شوند و کلیدهای رمزنگاری به‌صورت متمرکز و با دسترسی محدود مدیریت می‌شوند. معماری به‌گونه‌ای طراحی شده که حتی در صورت دسترسی غیرمجاز به یک بخش، امکان دسترسی به کل داده‌ها وجود نداشته باشد.

تفکیک محیط‌های توسعه، تست و تولید یکی از اصول کلیدی است. داده‌های واقعی کاربران هرگز در محیط توسعه استفاده نمی‌شوند و برای تست، داده‌های ساختگی یا ناشناس‌شده به‌کار گرفته می‌شوند.

سیاست نگهداری داده(Retention Policy)

یکی از مهم‌ترین بخش‌های این سند، سیاست نگهداری داده است. نگهداری بیش از حد داده نه‌تنها ارزش اضافه‌ای ایجاد نمی‌کند، بلکه ریسک را افزایش می‌دهد. در Metrogo برای هر نوع داده، بازه زمانی مشخصی تعریف شده است.

داده‌های مرتبط با تراکنش‌ها تا زمانی که الزامات قانونی و حسابداری ایجاب می‌کند نگهداری می‌شوند. پس از پایان این دوره، داده‌ها یا حذف می‌شوند یا به‌صورت غیرقابل بازگشت ناشناس‌سازی می‌گردند. داده‌های کاربران غیرفعال نیز پس از گذشت مدت مشخصی پاک‌سازی می‌شوند تا از انباشت داده‌های بلااستفاده جلوگیری شود.

فرآیند حذف و حق فراموش‌شدن

Metrogoبه حق کاربران برای حذف داده‌های خود احترام می‌گذارد. فرآیند حذف داده‌ها به‌صورت سیستمی طراحی شده و شامل حذف از دیتابیس اصلی، بکاپ‌ها و سیستم‌های تحلیلی است. این فرآیند مستندسازی شده و قابل پیگیری است تا در صورت نیاز به ارائه شواهد قانونی، امکان اثبات اجرای آن وجود داشته باشد.

در مواردی که حذف کامل داده باعث اختلال در تحلیل‌های کلان می‌شود، داده‌ها به‌صورت ناشناس و غیرقابل اتصال به فرد نگهداری می‌شوند.

مدیریت دسترسی و کنترل نقش‌ها

در Metrogo هیچ فرد یا سیستمی دسترسی فراتر از نیاز خود ندارد. دسترسی‌ها بر اساس نقش تعریف می‌شوند و به‌صورت دوره‌ای بازبینی می‌گردند. این رویکرد باعث کاهش خطای انسانی و سوءاستفاده احتمالی می‌شود.

نقش‌های حقوقی Controller :وProcessor

Metrogoبه‌عنوان Data Controller مسئول تصمیم‌گیری درباره چرایی و چگونگی پردازش داده‌هاست. در مقابل، سرویس‌های ثالث که به‌عنوان Data Processor عمل می‌کنند، تنها مجاز به پردازش داده‌ها در چارچوب تعریف‌شده هستند. این تفکیک نقش‌ها در قراردادها و توافقنامه‌ها به‌وضوح مشخص شده است.

توافقنامه‌های پردازش داده(DPA)

Metrogoبا تمامی سرویس‌های ثالثی که به داده کاربران دسترسی دارند، توافقنامه‌های پردازش داده منعقد کرده است. این توافقنامه‌ها مشخص می‌کنند داده چگونه پردازش می‌شود، چه مسئولیتی بر عهده هر طرف است و در صورت بروز حادثه، فرآیند پاسخ‌گویی چگونه خواهد بود.

حقوق کاربران و شفافیت

کاربران Metrogo حق دارند بدانند چه داده‌ای از آن‌ها جمع‌آوری می‌شود و برای چه منظوری استفاده می‌شود. سیاست‌های حریم خصوصی به‌صورت شفاف در اختیار کاربران قرار می‌گیرد و امکان دسترسی، اصلاح و حذف داده‌ها فراهم است.

مدیریت ریسک و آینده‌نگری

این سند نشان می‌دهد Metrogo منتظر بحران نمانده است. تهدیدهای احتمالی شناسایی شده‌اند و برای هرکدام راهکار کاهش ریسک در نظر گرفته شده است. این رویکرد، Metrogoرا برای رشد، جذب سرمایه و ورود به همکاری‌های بزرگ آماده می‌کند.