Data Security and Protection Overview

At NextAfter, we understand the sensitivity of your donor and subscriber data—and we take our responsibility for it very seriously. For that reason, we utilize platforms and techniques that meet (and exceed) industry standards for security and privacy. We also have an Information Security Policy dictating the sensitivity level of various types of data, who on our staff can access each, and how it can be interacted with. In addition to the non-disclosure agreement NextAfter has with your organization, every employee undergoes a criminal background check, signs an NDA, and receives training around our security policies to ensure accountability and consistent data handling.

Data Security

Constituent data is the most sensitive level of data defined in our policy, which requires multi-factor authentication and defines a principle of least privilege. In this case, it means that only our CTO and data analysts have access to non-aggregated client financial data provided through these requests.

While data is in our possession, it's encrypted both in transit and at rest (FIPS 140-2 certified), including the initial load and processing. Data is partitioned across multiple physical drives to ensure that no single drive contains any usable data. Once loaded into our data warehouse, it is also double (envelope) encrypted with a secondary key. The platform has several standards certifications, including PCI-DSS 3.2, HIPAA, ISO 27001, ISO 27017, ISO 27018, NIST 800-53/173 (certified for government use). All data is stored in client-specific datasets (not mixed with other organizations).

Data Use and Retention

You can also know that any data provided is used solely for its stated purpose (in this case, program analysis, dashboard creation, and audience segmentation). Any use other than the original purpose would require written permission from your organization. If NextAfter's services are ever terminated, all associated data will be securely deleted from your data warehouse.

If there are specific concerns around certain fields being provided, we're happy to discuss their use and necessity. Be aware, though, that the exclusion of certain fields can affect what we're able to analyze (e.g. email address which is used as a semi-unique key for aligning data from the email system with donor data to evaluate program performance and ROI). Omitting other fields, such as name and phone number, will reduce the accuracy of certain segmenting use cases such as anonymous/hashed matching in Facebook Custom Audiences (if permission for that case were granted in writing).

At the end of the day, our goal is to provide the best analysis possible, and due to the nature of exploratory analysis we often don't know exactly which data will end up being meaningful—which is why we ask for as complete a dataset as possible. **Your data remains <u>your</u> data and will <u>not</u> be shared with other nonprofits.**

Providing Data

To ensure the secure handling of constituent data, we recommend uploading them through our secure client portal (your unique link to which has been provided separately). If there's another way you'd like to provide the data (e.g. SFTP, a secure storage bucket, etc.), we're happy to discuss alternative options—we will not, however, accept sensitive data through non-encrypted channels (e.g. email).