Momentum Security Practices

Safeguarding the data of the charities Momentum works with and their donors is critical to our business. This document describes some of the security practices we use to make sure your data is safe in our care.

How and why we use data

We use data from your donor database so that we can make recommendations on how to connect with your donors, and help you act on those recommendations. We store data on your donors and their donations so that we can make these recommendations as helpful as possible. However, **we will never sell your data** under any circumstances.

How we protect your data

Momentum's database and web portal are hosted on leading cloud computing providers with best-in-class security, including Amazon Web Services and Google Cloud. Your data is encrypted at rest with industry standard AES-256 encryption, and access to our web portal is secured with TLS 1.2 encryption. Our donation platform uses Stripe, a PCI Level 1 certified payment processor.

Our web portal uses the Django web framework, which includes strong protection against cross site request forgery, SQL injection, and many other forms of attack. Our database and web application are further protected with Row Level Security, an advanced database feature that ensures that data from your organization can never be accidentally exposed to other organizations we work with.

Certain Momentum employees need access to your data in order to provide our services - for example, to review donor activity and recommendations. Access is tightly restricted to a small set of authorized personnel, and we have automated logging and auditing systems in place to ensure data is not improperly accessed. In addition, we require all employees with access to sensitive systems to use strong random passwords stored in a secure vault.

If you have any questions about our security practices, please contact our head of engineering: victor@givemomentum.com.