DigitalGenius cares about the security of its platform and your data. We operate a highly secure platform while addressing all relevant legal, industry, and regulatory concerns.

Yet everybody says that, don't they? Our security program is what sets us apart. It is based on three principles:

## Principle 1: We Don't Just Rely on AWS

AWS is great. It includes a comprehensive set of infrastructure security controls, and provides a strong foundation to build from. It has a rather impressive set of security compliance certifications, and is well-tested in the everyday battleground of malicious actors vs. the good guys.

Yet to build a secure platform within AWS requires extra work. AWS doesn't control what we do, nor how we deploy and implement our services. So we developed a comprehensive security program of our own, which includes controls at every corner of our world within the AWS cloud. To prove it, we embarked on our own, independent compliance program, which stands apart from and in addition to what AWS provides. DigitalGenius is GDPR compliant, undergoes annual SOC 2 reviews, and is aligned with ISO 27001, the gold standard for security governance; we will be certified under ISO 27001 in early 2019. DigitalGenius regularly engages third parties to perform testing of our security, including vulnerability scanning, penetration testing and code reviews.

## Principle 2: We Stick to Principles

All this compliance stuff is great, but let's be honest: when it comes to security, you care about how we think. At DigitalGenius, we aim to live by golden principles of security, such as:

***Data is only kept where it is absolutely needed for the time that it is needed, and no more.*** Roles are well-defined and access is driven by business need, not seniority. We keep everything updated all the time, in all the places, and keep things simple by relying on tightly defined containers instead of unnecessarily managing operating systems. We repeatedly test everything under our control, which means not just checkbox "network/web application pentests", because our core platform has nothing to do with web apps; we try to do things like break our APIs and leak data across customer boundaries. Our secure coding training is based on an actual secure code review of our own code, so that when the trainers talk to our developers, they can use examples from their own code.

## Principle 3: the Shared Responsibility Model

Just as in the case of AWS itself, DigitalGenius is responsible for maintaining a secure platform, managing all aspects of the platform to a high, secure, reliable standard; as our customer, you are responsible for using the DigitalGenius platform in a legal and responsible manner.

It is important to understand that as a platform, DigitalGenius has certain attributes that as our customer, you must take into account as you use our platform:

- DigitalGenius is data-neutral - we do not know, nor dictate, what data you choose to send to our platform. Our engine will process data you send to us on your behalf, based on your instructions as you configure the platform to perform your desired operations.

- DigitalGenius is data-agnostic - we treat all your data equally and confidentially. As the data controller, which data you send to our engine for processing is completely up to you.

- To support the use of the DigitalGenius platform in a responsible manner, it is important to follow security best practices: if any data is not required for training the AI engine, then it should not be sent to DigitalGenius.