GDPR Compliance for Online Identity Verification

"People come to me and say, 'How do I achieve GDPR compliance?'
... Start with PCI DSS."

JEREMY KING, INTERNATIONAL DIRECTOR AT THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL (PCI SSC)

Jumio's identity verification solution enables compliance across 5 critical aspects of GDPR:

1. Human Review

GDPR gives data subjects (i.e., your online customers) the right not to be subject to decisions solely based on automated processing that produce 'legal effects' or other significant effects.

Since Jumio takes a hybrid approach to online identity verification, combining machine learning, AI, computer vision, and biometrics, coupled with human review, we're able to provide much greater transparency about the rationale for acceptance or rejection for any given identity verification transaction.

2. Compliant Machine Learning

With GDPR, vendors can only develop specific AI models trained on the data of a given customer and cannot leverage data from other customers to create more comprehensive models.

Jumio's compliant machine learning approach builds in data privacy and security at every stage of the machine learning workflow including initial data capture, ID preprocessing, data tagging, algorithm training, and model deployment.

3. Data Retention

GDPR requires that personal data should be 'limited to what is necessary for the purposes for which they are processed,' and requires personal data storage being 'limited to a strict minimum.'

Because Jumio is PCI DSS compliant, we are already mandated to adhere to strict data retention procedures ensuring that personal data that is no longer needed is discarded appropriately and in a timely fashion. Our enterprise customers can customize data retention policies based on their unique business needs.

---

4. Breach Notification

GDPR requires data processors to notify the controller 'without undue delay' once aware of a data breach.

As part of Jumio's PCI DSS compliance, we regularly test our notification processes and procedures for dealing with data breaches. This ability helps our business customers manage their own breach notification and mitigation processes.

5. Data Encryption

GDPR requires data processors to have 'appropriate' measures to ensure security of personal data, including encryption, ensuring confidentiality, restoring data access and regular auditing/testing.

All personal data, including ID documents and selfies is encrypted twice: all data is encrypted in transit via TLS encryption using strong cipher suites and at rest with military-grade 256 bit AES encryption.

Chapter 4, Section 1, Article 28.1 states: ...the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.