GDPR & ONLINE IDENTITY PROOFING:

An Inconvenient Truth

Why Organizations Need to Vet Their Data Processors

FINTRAIL

jumio®

Preface

GDPR is just around the corner and many companies around the globe are busy implementing the necessary policies and procedures to ensure customer data is appropriately handled. At the time of this writing, however, over half of U.S. companies do not appear ready for GDPR compliance[1].

While it is the duty of all companies to ensure they properly protect and manage the data of EU citizens, this is especially important for companies offering identity verification solutions. Data processors in this space handle vast amounts of sensitive, personal data that, while integral to ensuring customers are who they say they are, can also be exploited or mishandled.

At the same time, the best data processors in identity verification can not only meet GDPR requirements, but also help collectors reduce their compliance burden.

This is why GDPR compliance is so important in the identity space. Data controllers need to make sure their processors, especially in the identity verification space, are being held accountable to a high standard when it comes to GDPR, in both the letter and spirit of the law.

We believe that the 5 key questions outlined in this e-book are the best way to frame your thinking about whether a data processor is effectively managing and exceeding the standards laid out in GDPR.

Hopefully, you will find the guidance in this e-book both informative as well as actionable in achieving the best results in customer protection and data security.

GEMMA ROGERS,
CO-FOUNDER, FINTRAIL

FINTRAIL

[1] CompTIA Research, April 2018

Introduction

More than a decade ago, *An Inconvenient Truth* was released as a documentary film featuring former U.S. Vice President, Al Gore, who makes his case to educate citizens about climate change and global warming. *An Inconvenient Truth* acted as a wake up call to raise public awareness of these issues and called for immediate action to curb destructive effects on the environment.

Similarly, GDPR represents a significant sea change in terms of data privacy and data protection—designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy.

Unfortunately, countless organizations, both inside and outside the EU, are completely unaware that GDPR applies to them and their third-party solution providers who handle personal data. In fact, GDPR applies to any business that holds data about or markets to persons within the EU.

Organizations that rely on third parties like Jumio for online identity verification need to understand that data processors represent an immediate and potential liability. Under GDPR, data subjects can bring claims directly against data controllers (any organization that collects personal information about EU citizens) and data processors. Every data controller and data processor can be held liable for the damage suffered by a data subject as a result of non-compliance, and can be ordered to effectively compensate the data subjects involved.

When one considers the financial, regulatory, and reputational risks, it's no wonder why so many organizations are scrambling to reduce their compliance exposure.

GDPR comes into effect on May 25, 2018 and this e-book was written to provide actionable guidance on how to determine if a selected data processor is, in fact, fully compliant. Given the regulatory focus on enforcement and the hefty fines involved, companies have too much at stake to blindly accept the claims of data processors that they are GDPR compliant. To protect themselves and their customers, companies need to ask processors the right questions such as how they are compliant and how their processes are vetted.

This e-book provides valuable guidance to help companies vet their data processors for GDPR compliance.

Let's get started.

What is GDPR?

GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens. It aims to protect the "personal data" of EU citizens—including how the data is collected, stored, processed, and destroyed. If an organization is based in the EU or conducts business with EU citizens, GDPR applies.

Who is Impacted?

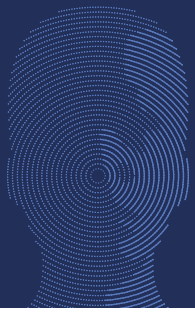
The provisions of GDPR are consistent across all 28 EU member states, which means that companies have just one standard to meet within the EU. However, that standard is quite high and will require most companies to make a large investment to meet and to administer.

But, this isn't just a regulation confined to EU companies. It's a growing concern for non-EU based companies too. GDPR also applies to processors and controllers not established in the European Union who provide goods/services to citizens of the EU or who monitor behavior taking place in the EU. There is considerable concern that companies located outside the EU do not realize that they are subject to GDPR requirements. Organizations can take this self assessment questionnaire, sponsored by the Information Commissioner's Office (ICO), to assess their progress with GDPR compliance, whether they're data controllers or data processors.

According to an Ovum report, about two-thirds of U.S. companies believe GDPR will require them to rethink their strategy in Europe. In fact, 85% of those surveyed see the GDPR putting them at a competitive disadvantage with European companies.

GDPR's Definition of Personal Data

The meaning of "personal data" under GDPR goes far beyond what you might expect considering how similar terms are defined in the U.S. Under GDPR, "personal data" means information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. This even includes IP addresses, cookie strings, social media posts, online contacts, and mobile device IDs.



Data Processors vs. Data Controllers

An important distinction is made in GDPR between data processors and controllers:

Controllers
determine the purposes and means of the processing of personal data.

Processors
process personal data on behalf of the controller.

While data controllers are more directly targeted by GDPR and held to stricter requirements (e.g. specific data breach reporting periods) and are responsible for managing consent to process PII data, processors are still expected to meet GDPR requirements and to follow the instructions of the controller.

> *Chapter 4, Section 1, Article 28.1 states: ...the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational 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.*

But, data processors also carry some important obligations. In particular, GDPR expressly provides that the data processor:

- only acts on the data controller's documented instructions, unless Union or Member State law to which the processor is subject, determines otherwise;
- imposes confidentiality obligations on all personnel involved in processing the relevant data;
- ensures the security of the personal data by implementing the measures;
- abides by the rules regarding the engagement of sub-processors (prior authorization needed of the controller and sub-processors must be appointed on the same terms as are set out in the contract between the data controller and the data processor);
- assists the data controller, where possible, with implementing measures to comply with the rights of data subjects;
- assists the data controller in obtaining approval from the relevant DPAs;
- at the data controller's request, either returns or destroys the personal data at the end of the agreement (except as otherwise required by Union or Member State law); and
- provides the data controller with all information necessary to demonstrate compliance with GDPR.

To best achieve GDPR compliance and to establish a strong partnership, processors and controllers must have a jointly-developed strategy in how they process and handle the data of their customers and users.

GDPR & Online Identity Verification

Since online services are here to stay and as the general population turns to the Internet for their ever increasing needs, knowing who's who is becoming imperative. For many industries, companies have to establish trust and connect a person's online identity with their real-world identity. This type of online identity verification is often outsourced to solution providers like Jumio and it's critical to note that GDPR imposes strict requirements on any vendor that is managing personally identifiable information (PII), including images of government-issued IDs, biometrics, and other personal information.

GDPR acknowledges the importance of establishing and protecting digital identity and that's why it is imperative for identity verification providers to compliantly secure the information they capture, and at the same time, make its use clear, easy-to-understand, and transparent to the individual.

If a company is using an online identity verification solution, they need to make sure that once they have gathered the data (e.g., a picture of the government-issued ID and selfie), they tell the customer what they will do with it. Will the data be deleted or kept? If kept, for how long and what measures have been taken to safeguard it? All of this needs to be done with the clear consent of the individual in concern and the individual should have the right to delete their data if they choose to do so.

That said, the GDPR leaves much to interpretation. The regulation states that companies must provide a "reasonable" level of protection for personal data, for example, but it does not define what constitutes "reasonable." This gives the GDPR governing body a lot of leeway when it comes to assessing fines for data breaches and non-compliance.

5 Critical Questions to Ask Your Data Processor (Online Identity Verification Provider)

Business customers who use an online ID and identity verification solution will often be considered data controllers under GDPR. Under these circumstances, customers should look to their verification provider to demonstrate its ability to meet and where possible, simplify, the company's GDPR compliance objectives.

And since the identity verification solution provider will be listed as a third party in possession of the subject's data under GDPR, businesses have an added incentive to choose their vendor wisely. Given the important intersection between identity verification and GDPR compliance, it is important to understand what to look for in an online identity verification solution.

Our recommendations are summarized in these 5 questions:

How are verification decisions made and what recourse do data subjects have to challenge those decisions?

GDPR Requirement

Chapter 3, Section 4, Article 22.1 gives data subjects the right to not be subjected to decisions solely based on automated processing that produces 'legal effects' or other significant effects.

Impact on Identity Verification

As more online verifications are carried out by algorithms, concerns have been raised about the lack of transparency behind the technology, which leaves online customers with little understanding of how decisions are made about them. Many automated solutions include no human review, and several hybrid providers only provide human review for a small subset of verifications. With GDPR, how your digital identity verification provider performs these verifications becomes important to maintaining compliance.

Under GDPR, an individual can request information (known as Subject Access Requests) about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret). Data controllers must be able to address GDPR's requirements for a data subject's right to explanation (Article 13) and respond to Subject Access Requests within 30 days. This means that data processors must be well equipped and have the reporting mechanisms in place to help controllers meet these tight deadlines.

Key Questions to Ask:

- Can the data processor support the data controller by providing sufficient transaction details within 30 days?
- Specifically, how are IDs and identities being verified?
- Are human experts involved in making the verification decision?
- When an identity or ID is rejected, how granular is the rationale?
- Can the data processor provide a complete explanation for a specific verification (per a data controller request)?

Does the data processor employ Compliant Machine Learning?

GDPR Requirement

Chapter 3, Section 4, Article 22.1 gives data subjects the right not to be subject to decisions solely based on automated processing that produces 'legal effects' or other significant effects. However, GDPR is not specific about how data processors can apply machine learning algorithms. Some of the articles of GDPR can be interpreted as requiring explanation of the decision made by a machine learning algorithm, when it is applied to a human subject.

Impact on Identity Verification

Many identity verification vendors aggregate data across multiple customers to develop their machine learning algorithms. 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. Moreover, Compliant Machine Learning models must build 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.

Key Questions to Ask:

- Does your identity verification methodology incorporate machine learning?
- If so, how are your models created (e.g., built on data across customers)?
- Post GDPR, how will your machine learning models change (if at all)?
- Is your verification facility locked down in terms of physical security and are smartphones or thumb drives allowed within the verification facility?
- Is PII data encrypted whenever it is sent via the API?

Can your data retention policies be tailored to your business requirements?

GDPR Requirement

Clause 39 states that personal data should be 'limited to what is necessary for the purposes for which they are processed,' which, it furthers, requires personal data storage being 'limited to a strict minimum.'

Impact on Identity Verification

In addition to addressing the limitations around personal data, business customers must also consider the requirement to retain sufficient transaction history in order to respond to subject access requests (within 30 days) and to retain the ability to correct inaccurate customer data (Article 16). So, it's imperative that identity verification providers have clear processes around data retention and deletion, and as we've stated previously that they are set up to help controllers process subject access requests appropriately.

Key Questions to Ask:

- Can you customize your data retention policies to satisfy your business requirements?
- Can you easily satisfy subject access requests?
- How is personal data securely and compliantly deleted?

Do you have a data breach notification process in place and has it been tested?

GDPR Requirement

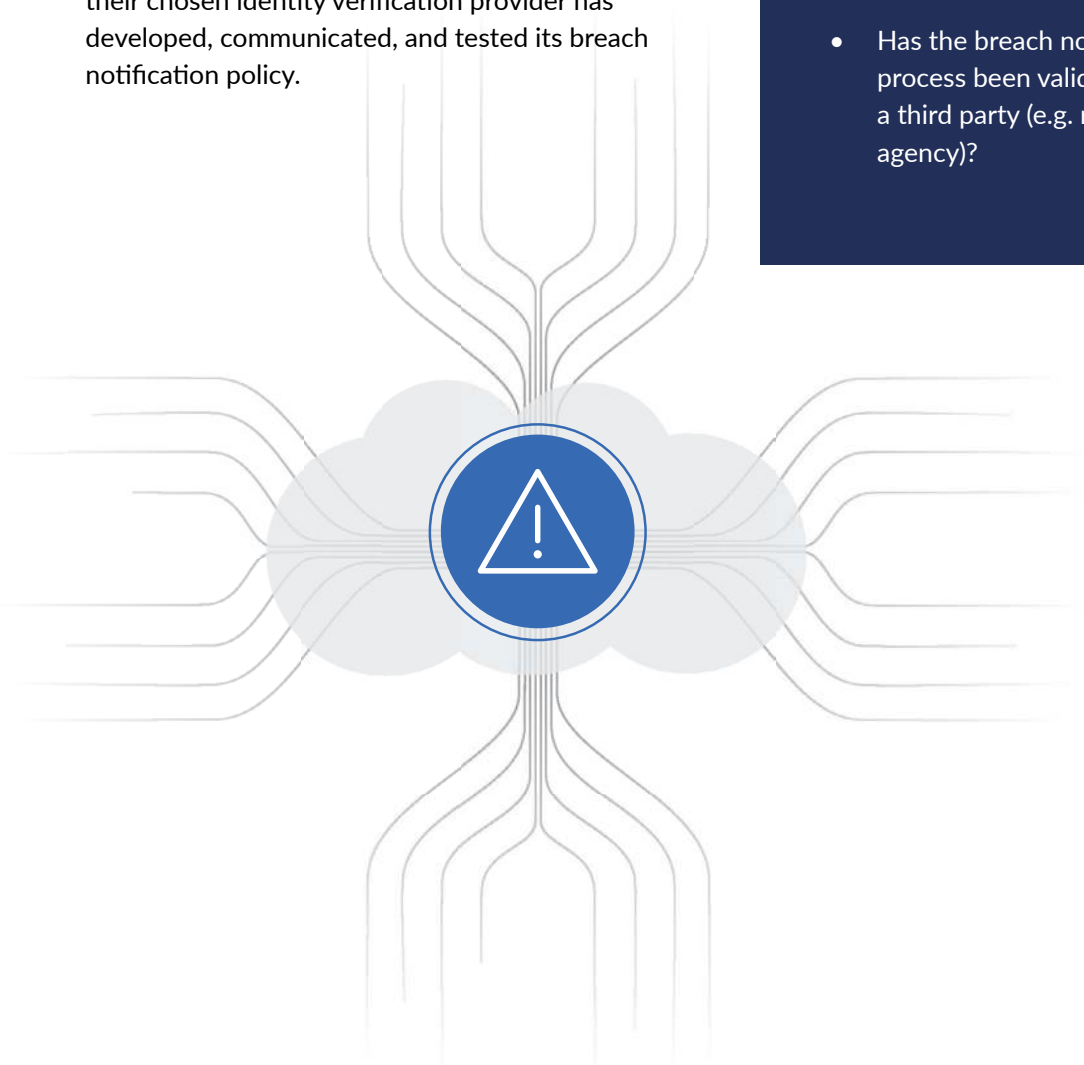
Chapter 4, Section 2, Article 33.2 requires the processor to notify the controller 'without undue delay' once aware of a data breach.

Impact on Identity Verification

Many identity verification vendors lack established or tested processes for data breach notifications. Customers should have the reasonable expectation that any company they transact with online has the ability to detect a breach, and just as important, that they will be notified of the breach in a timely fashion. Data controllers should understand how their chosen identity verification provider has developed, communicated, and tested its breach notification policy.

Key Questions to Ask:

- Do you have a data breach notification process?
- Has the process been documented in writing and communicated to all of your employees?
- Has the process been thoroughly tested and put through its paces?
- Has the breach notification process been validated with a third party (e.g. regulatory agency)?



How is personal (PII) data encrypted and protected?

GDPR Requirement

Chapter 4, Section 2, Article 32.1 requires controllers and processors to have 'appropriate' measures to ensure the security of data processing, including pseudonymisation and encryption, ensuring confidentiality, restoring data access, and regular auditing/testing.

Impact on Identity Verification

Proper data protection and encryption reduces the likelihood of a breach and increases the privacy of citizens' information. As a data processor, it's vital to build trust through regulated status and thorough testing and assurance. Solution providers must address how data is captured, transmitted, and stored. This affects things like how data is encrypted in transit and at rest, and how much logging and auditing of systems is available at the processor's end.

Key Questions to Ask:

- How are ID documents being encrypted upon capture?
- How are those documents encrypted in-transit to the data processor?
- How is the data encrypted at rest (within the data processor's data centers)?
- What type of risk assessments have been performed?
- Have these encryption processes been vetted by a third party?

Key Takeaways

Rather than just accepting a data processor's claim that they are GDPR compliant, it's important to peel back the onion to understand:

1. How automated are their solutions and do your customers have actionable recourse?
2. Have they deployed Compliant Machine Learning and built in privacy and data protection into every step of the workflow?
3. Do they have configurable data retention policies?
4. Do they have written, tested, and vetted data breach notification plans in place?
5. How do they address data security and encryption?

Understanding their answers to these questions will help you sleep a little easier at night knowing that your data processors are not just GDPR-compliant, but also GDPR enablers positioned to help you tick all the regulatory boxes as well as reduce your organization's financial, regulatory, and reputational risk exposure.

Understanding Data Subject Access Requests

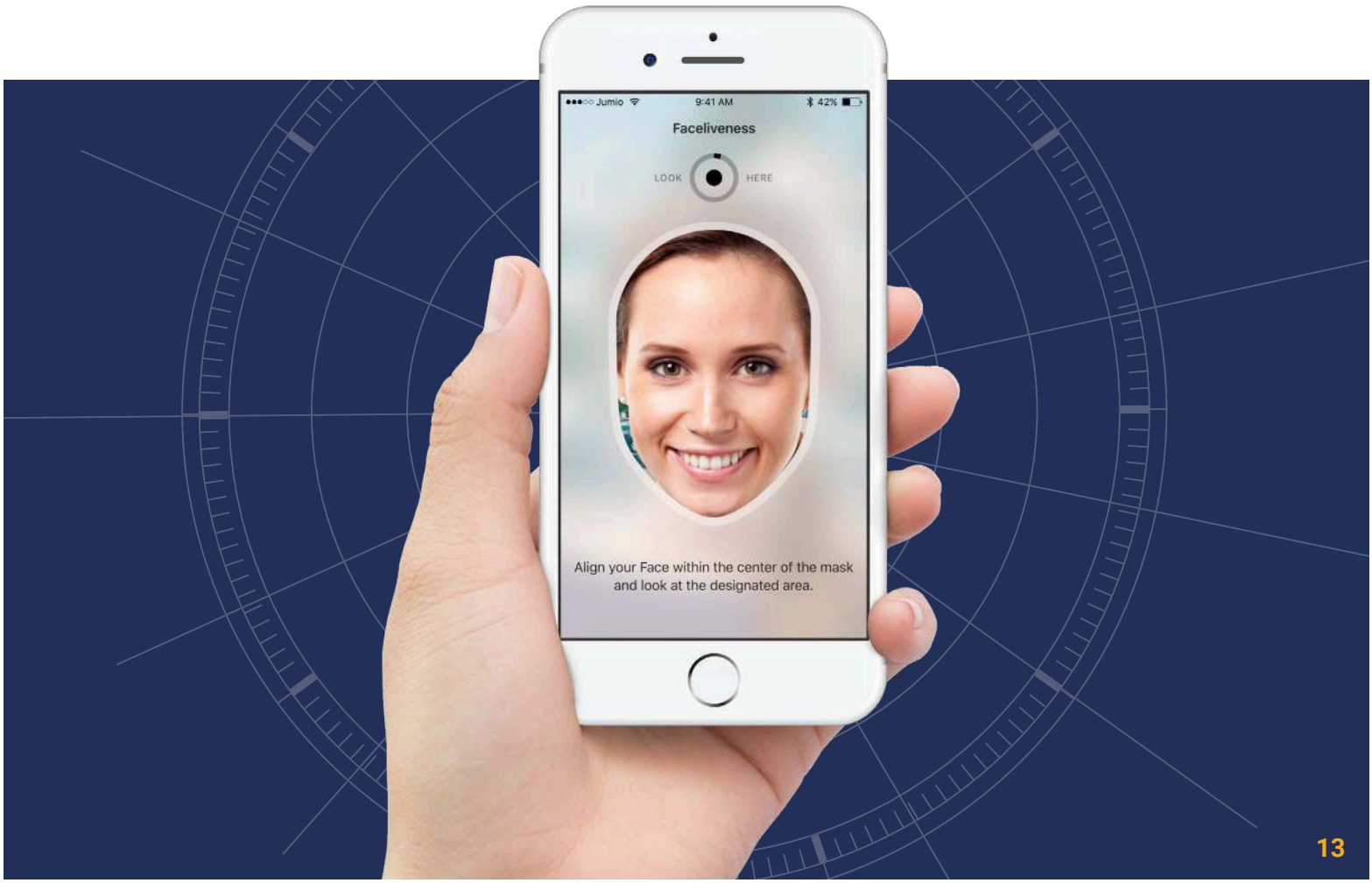
Data subjects under GDPR have the right to file a data subject access request (DSAR). This means that data subjects have the right to obtain confirmation about whether their data is being processed, the purposes of the processing, the categories of data being processed, its recipients, where the data is being stored, whether it is part of an automated profiling process, and the data itself. It is the responsibility of the data controller to respond to these requests within the 30-day time limit. Processors are expected to assist data controllers however needed with responding to DSARs, as the time limit is not extended for controllers who are using processors.

How Jumio Satisfies GDPR's 5 Must-Haves

Jumio takes privacy and data security seriously, but this claim will be echoed by most data processors. How can data controllers have more confidence that their chosen data processors are actually complying with all of GDPR's relevant requirements—both in terms of the letter and the spirit of GDPR?

Jumio's Commitment to GDPR

Jumio is not only fully GDPR compliant as a data processor, with a robust and transparent program for maintaining all standards laid out in GDPR, but its identity verification product is a key GDPR enabler, offering business customers the ability to maintain data protection and contribute to compliance with GDPR requirements.



Let's address how Jumio meets each of the 5 core ingredients of GDPR that explicitly impact online identity verification.

Human Review

The Requirement

As increasingly more online verifications are carried out by algorithms, concerns have been raised about the lack of transparency behind the technology, which leaves consumers with little understanding of how decisions are made about them. Profiling and fully automated decisions are only allowed with express consent of the subject, when authorized by EU or member state law, or as part of a contract. Legitimate interest does not count as a reason for fully automated decision making (as explained by the Article 29 Data Protection Working Party, or WP29). Solutions with some human review element are more permissible.

Article 13 states that individuals have the right to a clear explanation of the logic behind data processing (included automated processing). ID document and biometric (selfie) data are often used by FinTechs and other customers to develop automated risk engines or machine learning-based customer risk monitoring tools that must be ensured to be GDPR compliant.

GDPR gives data subjects (i.e., online customers) the right not to be subject to decisions solely based on automated processing that produces 'legal effects' or other significant effects. Data subjects can request access to information on how their data is being used at any time. Having a human review element will help data processors provide a more timely and usually, a more thorough explanation, for any rejected transaction and help data controllers more quickly follow up with data subject access requests.

How Jumio Satisfies the Requirement

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

Compliant Machine Learning

The Requirement

There is considerable confusion around GDPR and its overlap with machine learning. So, it is important to make sure the spirit of GDPR is honored. The biggest controversy relates to 'right to explanation' as machine learning is incredibly complex and difficult to explain.

If machine learning models are used, data subjects have a 'right to explanation' of how their data will be used in the models. This means simplifying the rationale of why data needs to be processed through machine learning (to best identify suspicious customer traits linked to financial crime) as well as a simplified and clear explanation of how the machine learning model functions.

Recital 71 states automated processing "should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision." So, while machine learning can be used, it should still be done so within the confines of other tenets of GDPR.

This also touches on data subjects' right to disappear, as you would need to be able to remove their data from the machine learning process if requested. The data minimization principle also comes into play. How necessary is it to keep and maintain customer data for machine learning? Can your objectives be achieved another way? Based on legal counsel, our interpretation of GDPR (at least in terms of the spirit of the law) is that processors cannot commingle data from multiple customer sources to aggregate data for machine learning. GDPR doesn't make machine learning illegal, but there is a lot of ambiguity, and it has become more difficult to manage.

Many identity verification vendors aggregate data across multiple customers to develop their machine learning algorithms. It's Jumio's position that online identity verification 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.

How Jumio Satisfies the Requirement

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.

Data Retention

The Requirement

Simplified data retention is critical to improving data security and data protection measures by reducing the surface area of exposed data. It is also important in trust-building between all players in the data lifecycle. Being able to customize data retention is useful in improving flexibility and capacity to meet GDPR requirements under different circumstances. 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 to be 'limited to a strict minimum.'

How Jumio Satisfies the Requirement

Because Jumio is PCI DSS compliant, it is 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. Jumio's enterprise customers can customize data retention policies based on their unique business needs.

Data Breach Notifications

The Requirement

Breaches can cause serious legal, financial, and reputational repercussions if not handled swiftly, efficiently, and securely. Processors under Article 33.2 must inform controllers of breaches ASAP, and then the controller has 72 hours to report a breach to the ICO (or comparable data protection agency outside of the UK). More precise variations on breach notification will be determined in the controller/processor contract. If a breach will result in a high risk to the rights and freedoms of individuals, those individuals will have to be informed ASAP and in clear and plain language. Failure to comply can result in a fine up to 10 million euros or 2 percent of global turnover (revenue), whichever is greater.

How Jumio Satisfies the Requirement

Many identity verification vendors lack established or tested processes in place for data breach notifications. Because Jumio is already PCI DSS compliant, it regularly tests its notification processes and procedures for dealing with data breaches. This ability helps Jumio's business customers manage their own breach notification and mitigation processes.

Data Encryption

The Requirement

Data processors need to reduce the impact that data will be breached by using state-of-the-art security measures. This means encrypting data throughout the entirety of the data's lifecycle—and the level of data protection being used needs to be clearly communicated as well. GDPR also considers it a best practice to audit how encryption is performed.

GDPR requires data processors to have 'appropriate' measures to ensure the security of personal data, including encryption, ensuring confidentiality, restoring data access, and regular auditing/testing. Risk assessments of new processing and new products should be used to understand the data encryption and security measures that will be necessary for GDPR compliance.

How Jumio Satisfies the Requirement

Because Jumio is PCI-DSS Level 1 compliant, it regularly subjects its security practices to stringent regulatory security audits, vulnerability scans, and penetration tests to ensure compliance of the product. 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.

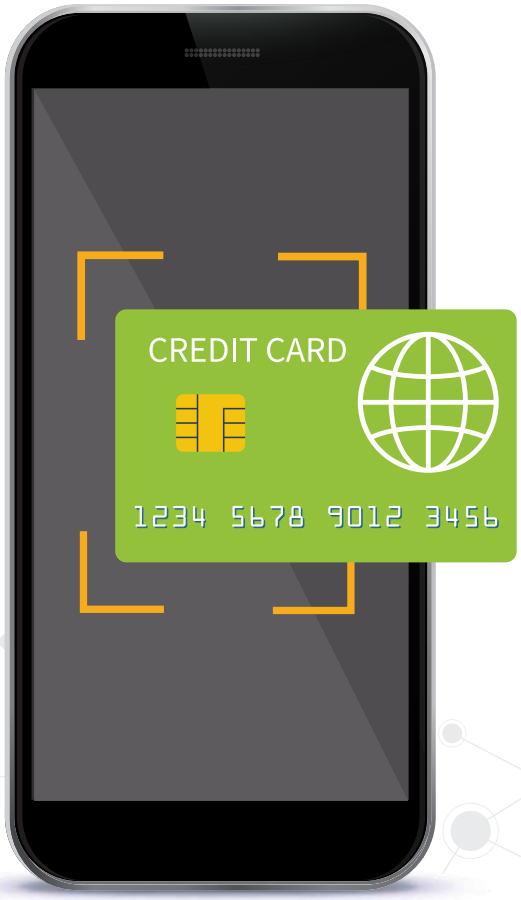
The Looming Importance of PCI DSS

> “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)

Both PCI DSS and GDPR are designed to improve customer data protection. PCI DSS focuses on payment card data whilst the GDPR focuses on personally identifiable information. However, despite the clear overlap, there are significant differences in terms of how the two are phrased.

The good news for organizations already PCI DSS compliant is that the GDPR is less prescriptive than the PCI DSS standard. The GDPR lays out what organizations need to do but does not spell out precisely how. In contrast, PCI DSS not only specifies what needs to be achieved but also how it should be achieved, with regular updates and a clear methodology for achieving card data security that the GDPR lacks.

This means that if an organization is compliant with the PCI DSS, it is probably already meeting the baseline security control standards of the GDPR. That’s why data processors that are already PCI DSS compliant have a big head start on implementing the kinds of data security best practices and controls that the GDPR requires.



Jumio is ahead of the game.

Jumio is one of the only verification solution providers to achieve PCI compliance by having its policies, processes, and controls independently tested to ensure that customer's data—be it credit card or PII—is handled in a secure manner throughout its lifetime. This means that Jumio already has established and vetted procedures for data encryption, data retention, and data breach notifications—addressing three of the five core ingredients outlined above.

Category	PCI-DSS Requirement
Data Encryption	• Encrypt data in transit and at rest • Security audits, penetration tests, vulnerability scans • Leverage industry-tested and accepted algorithms for cryptography • Render PAN unreadable anywhere it is stored (masking)
Data Retention	• Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes • Secure deletion of PII data
Data Breach Notification	• Created incident response plan • Evangelized plan internally • Regularly tested • Independently audited

Conclusion

A Symbiotic Relationship: Processors & Controllers

If you work with online identity verification platforms that capture personal data from data subjects in the scope of their job, they must follow the same GDPR rules and provide the data controller with the data and the records. It's clear that controllers have a responsibility with regards to the processors they work with, but that the processor also can be held liable in case of GDPR infringements that can lead to painful fines for non-compliance.

The inconvenient truth about GDPR, now upon us, is that your data processors play a pivotal role in your ability meet the strict guidelines for data privacy and protection—and in most cases, this starts with marrying the online identities of your customers to their real-life identities. Because of this important role, online identity verification solutions occupy a special place as a data processor and need to be fully vetted to ensure that any lapse in their data security and processes don't open up headaches, exposure, and legal liability on your end.

We hope this e-book equipped you with a helpful framework to evaluate your vendors and help ensure that they have all of their ducks in a row. By ensuring your data processor can address each of the 5 core ingredients to compliance, ideally from an outside accreditation (e.g., PCI DSS compliance), you're much better positioned from a security and compliance standpoint.

When it comes to GDPR compliance, you are only as strong as your weakest link—so make sure that you fortify all the links in the chain—both inside and outside your organization.

At FINTRAIL we provide our clients with access to a new, agile and energetic form of financial crime risk management. This requires a different approach, one that is not simply a box-ticking compliance process or a regulatory burden, but one that puts commerciality and intelligent risk management at its core, and something we believe is vital to businesses of any size.

www.fintrail.co.uk

Leveraging advanced technology including augmented AI, biometric facial recognition, machine learning, and human review, Jumio helps organizations to meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of its customers. Jumio has verified more than 120 million identities issued by over 200 countries from real time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, cryptocurrency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in the US, Europe, and Asia Pacific and has been the recipient of numerous awards for innovation.

www.jumio.com