GDPR by Design - Coalescing Privacy, Security and UX

Risk Mitigation, Pseudonmynisation and Data Minimisation

May 25, 2018 will mark the end of the current EU Data Privacy Framework and current e-Privacy rules. Will you seize the day or rue the day?

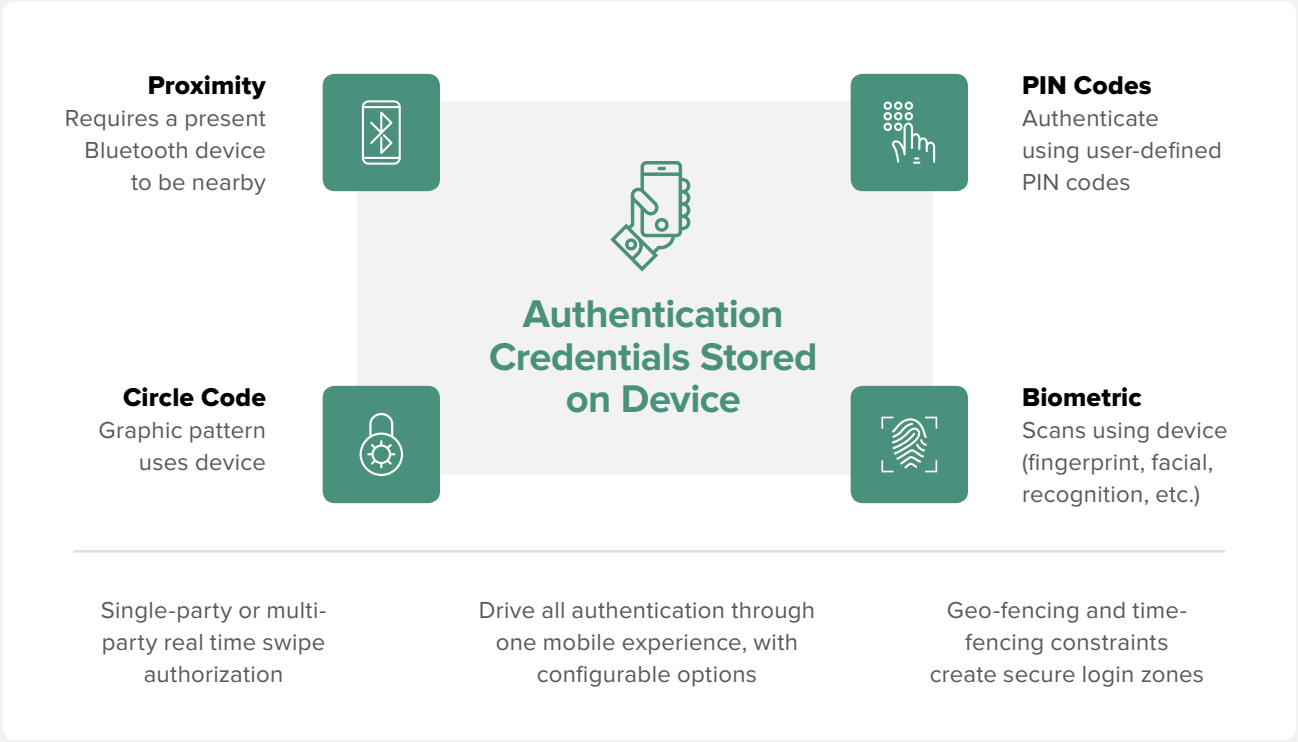
GDPR coalesces data privacy legislation from the EU28 into one regulation. It also includes potential fines for transgressors of over €20m or 4 percent of worldwide turnover, whichever is greater, that are globally enforceable. While the potential fines are sure to inspire heart palpitations, it's also an opportunity to rethink the customer relationship. To embrace consumer privacy rights in a way that provides a greater level of security while preserving or even improving the customer experience.

Reducing Data Breach Risks, Improving User Experience

With the constant threat of compromised credentials and brute force hacks, consumer brands need multifactor authentication to secure online accounts, but conventional solutions that store personal data on-prem or cloud-based servers can prove reputationally or materially damaging to a company if breached. This will be especially true in the new GDPR landscape.

LaunchKey, iovation's multifactor authentication (MFA) solution, provides a decentralized and anonymous architecture that stores authentication credentials locally on the user's device, and never creates the "central data store" that leads to the breaches we

How LaunchKey Works



read about in the news. This approach significantly reduces exposure if -- many experts say “when” -- a breach occurs.

Balancing security with user experience, LaunchKey also helps you provide a seamless omni-channel service for your customers. iovation’s lightweight SDK can be deployed through your own application, managing all digital and physical authentication and authorization processes. LaunchKey allows you to quickly authenticate good customers across multiple platforms, from today’s web or mobile app to tomorrow’s omni-channel experience across call centers, kiosks, ATMs and IoT devices. LaunchKey provides the broadest set of authentication methods and unifies customer experience utilizing configurable authentication options such as biometrics, geo-fencing, circle codes and Bluetooth proximity detection.

Fighting Cyber Criminals Under GDPR

Although data processed for Criminal Law enforcement purposes will be ring-fenced under its own directive across the EU (with the UK still as yet unclear as to their intentions), GDPR provides some call outs for counter fraud activity.

Data processing under GDPR requires a “condition of processing”. These range from a legal obligation to do something (e.g. government tax collection) through to the consent of the person involved. While it’s unlikely a fraudster would consent to having their personal details processed, organisations will be able to rely on their own legitimate interests to prevent fraud as a condition of processing (Article 6; Recital 47).

In addition, profiling for praud prevention is specifically called out as a permissible activity (Recital 71).

Data minimisation - Doing more with less

One of GDPR’s requirements is the principle of “data minimisation”, where an organisation only collects that data which is necessary for the intended aim. iovation’s solutions require the barest amount of non-invasive, non-directly identifying personal data to provide effective authentication and fraud prevention solutions. Because, even if a fraudster provided their details, we wouldn’t be inclined to believe them anyway. This means iovation’s solutions are perfectly positioned to help you shut down account takeover attempts and other types of fraud while staying compliant with GDPR.

Pseudonmynisation

The GDPR defines pseudonmynisation as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.”

With the implementation of GDPR in May 2018, iovation will enable organisations to leverage the benefits of pseudonymized data. Not only ensuring the security of data in the event of a breach, but also allowing Data Controllers to be exempted from notifying regulators and individuals in the event of a data breach (Article 33 GDPR - on the basis that securely pseudonymised data is “unlikely” to create risk). In addition, Article 11, which relaxes certain data subject rights for pseudonymised data, will assist businesses in dealing with the anticipated increase in the enforcement of Subject Access Rights. EU Justice Commissioner Vera Jourova recently announced her intention to launch a “massive” awareness campaign around the new rights that GDPR confers. As people become aware of these rights and that they may have a right to compensation for the impediment of those rights, you can be sure that there will be an increase in legal action.

Privacy Shield

In iovation’s commitment to ensure compliance with all data privacy and security regulations, we have undertaken a number of initiatives to meet the EU-US Privacy Shield standard, and are working towards self-certification to become Privacy Shield compliant in 2017. The EU-US Privacy Shield Framework was designed by the US Department of Commerce and European Commission as a replacement for Safe Harbor after it was invalidated by the EU’s highest court in 2015.

Privacy Shield enables US businesses to provide assurances that they can process data in line with the high expectations placed on their counterparts in the European Union. This enables businesses to operate in a far more agile manner by avoiding cumbersome contract negotiations and consumer consent isn't absolute when other conditions of processing are considered. This enables transatlantic data flows to persist, which are the lifeblood of globalised industry. It also ensures that downstream processing is carried out to the same high standard that is required of the "importer" of EU sourced data into the US.

What about Brexit?

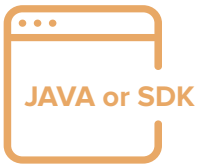
The United Kingdom submitted notice to the European Commission on 31st March 2017, which set in motion a two-year period of negotiation as prescribed by Article 50 of the Lisbon Treaty, during which the UK would be able to negotiate the withdrawal of its 44-year membership from the European Union. During this timeframe, all current and proposed EU legislation would become enshrined into UK law. As such, GDPR precedes the earliest possible time for Brexit to take place, and it will have been enacted for over ten months. At this point, under the proposed “Great Repeal Act”, it will be incorporated into the UK statute book. Whether the UK will then become an adequate “Third Country” under EU data privacy rules remains to be seen. Also complicating the picture is whether Brexit will be hindered by the UK’s “Hung Parliament” following the recent Election.

How iovation Collects and Processes Data

1

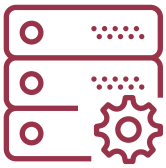
Customer visits your website or mobile app from any device

2



Device fingerprint and minimal amount of non-directly identifying data collected in 'blackbox' and encrypted

3



Blackbox sent to device intelligence platform for analysis

4

A real-time response is returned about the transaction

The new era of Privacy as a consumer right and a corporate social responsibility is dawning. Whether preventing fraud, or authenticating good customers, iovation can help your organisation in the journey to GDPR compliance without sacrificing the customer experience. Will you face significant financial penalties, get outpaced by your competition or seize the day?

iovation®

Ready to get started? ? For a free demo and to receive a consultation on preparing your business for GDPR, please visit https://www.iovation.com/demo or email us at info@iovation.com

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com