Paysafe

2018's Legislative Trifecta:

Changing the face of ecommerce

Challenge & opportunity for financial services

Contact us

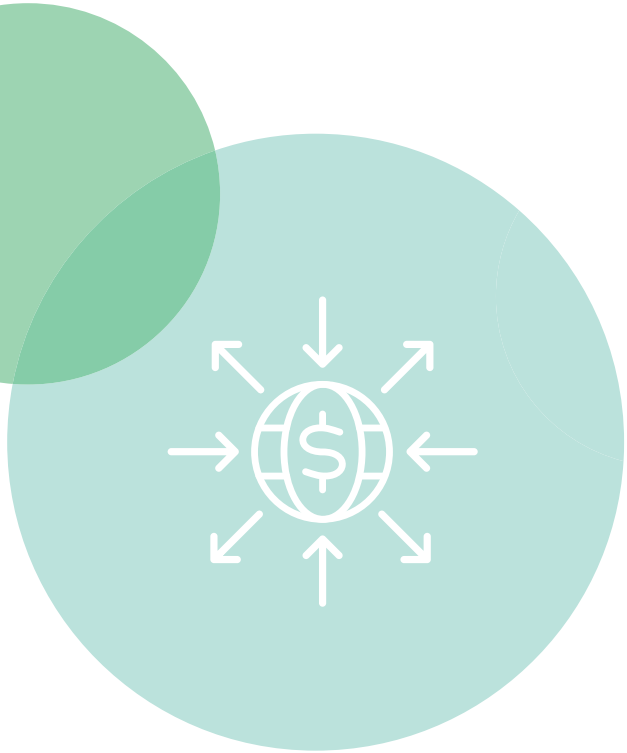
www.paysafe.com

pr@paysafe.com

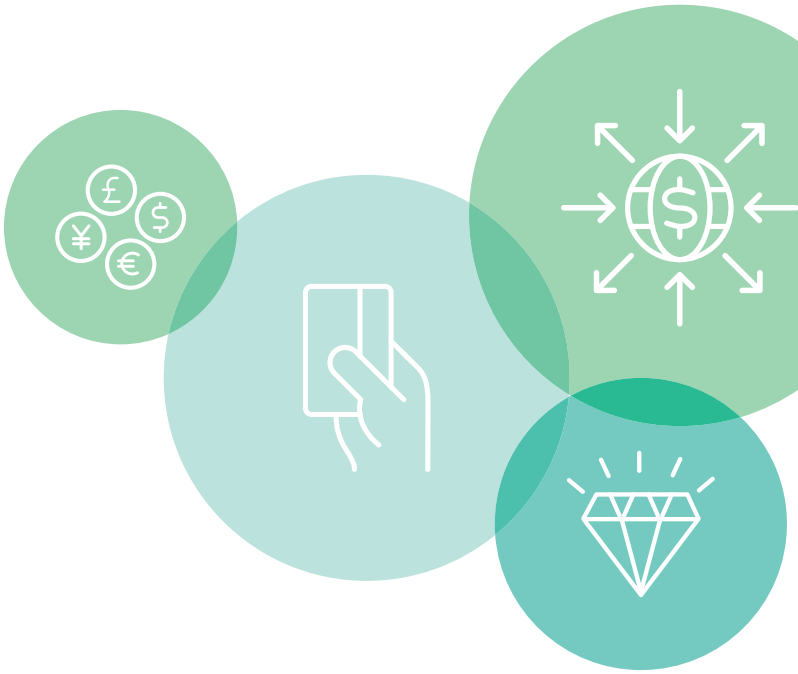
@PaysafeGroup

/PaysafeGroup

Paysafe



Contents



Executive Summary

The world's most valuable resource is no longer oil, but data.

In today's digitally transformed and connected world, data is produced in vast streams daily, at a mind-boggling volume and pace. A global 'rush' is now on to tap data flows and extract value. Not surprisingly, a heightened focus on data security and customer privacy has followed.

Focusing on security without privacy would be like having a house made of bullet-proof, transparent glass. Sure, no one will get inside, but your personal life is still on display to all.

Only by engineering security *and* privacy into the DNA of the next era of digital business can we hope to build a better place for future generations. This will not be achieved by accident, and the new legislative imperatives are now compelling.

To succeed in this new world, businesses will have an inherent appreciation of data protection and customer privacy, placing both at the very core of what they do.

A Legislative Trifecta

Three new intergovernmental regulations and mandates will fundamentally change the face of ecommerce in 2018. Compliance with this new raft of legislation is driving many businesses to re-design and re-engineer their operations. While originating from European Union (EU) policymakers, the Second Payment Services Directive (PSD2), the General Data Protection Regulation (GDPR) and the replacement e-Privacy Regulations all have a global impact due to their extra territorial reach over European citizens' data.

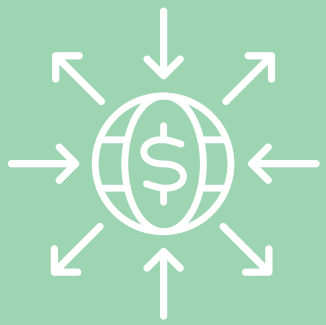
The **PSD2** legislation came into force in January 2018 with the intention to break down the monopoly that banks hold over user data and improve on PSD1 which came into effect in 2007. Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) will be now able to make payments for customers' goods and services once the user has granted appropriate permissions.

The forthcoming **GDPR** builds on the existing Data Protection Directive, which has been in place since 1995, and will impact businesses worldwide that have interests, holdings, customers and other touch points within the European Economic Area (EEA). The GDPR comes into effect on May 25, 2018 and extends the scope of EU data protection law to all foreign companies processing data that belongs to or relates to EU residents. The cost of non-compliance with this new regime has severe penalties of up to €20 EUR million or 4% of global annual turnover – whichever is greater.

The **e-Privacy Regulations** is separate legislation, currently in draft, which will replace the current e-Privacy Directiveand covers the consent requirements for cookies and electronic marketing. It will replace existing European Member State Regulations on the way companies collect and store data about customers and their electronic devices (such as computers, mobile phones, tablets, etc.) on-line and through their interactions with websites and mobile apps. Anticipated to be in effect by the end of 2018, it appears likely that the new consent requirements will be more onerous than existing requirements.

The big conundrum facing companies looking at GDPR and e-Privacy is that under GDPR the use of personal data for profiling and Online Behavioural Advertising (OBA) can normally rely on 'legitimate interests' as lawful grounds for processing. However, under the e-Privacy Regulations the use of cookies for profiling and OBA always requires *prior* consent from the individual.

Accordingly, the e-Privacy Regulations will change the way in which companies operate in the areas of on-line fraud detection and prevention, on-line based digital advertising, and the tracking of customers activity across websites and mobile apps.



Processing Personal Data: 7 Principles

An organisation's responsibilities under GDPR

1.	Lawfulness, fairness & transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject *This means organisations have to be absolutely clear with their customers about what they do with customer data.*
2.	Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes *This means if an organisation collects data for one purpose, it can only use that data for that specific purpose and not for any secondary reason or purpose that the customer hasn't been informed of.*
3.	Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *This means organisations should only be collecting the information needed to provide the service its customers have agreed on.*
4.	Accuracy	Personal data shall be accurate and, where necessary, kept up to date *This means organisations need to keep data clean and up-to-date so as not to have any negative impact on its customers.*
5.	Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed *This means organisations have to delete data in accordance with data retention policy, such as the 'Right to be forgotten' whereby a customer can compel a business to delete information held about them. However, in the case of financial services there may be regulatory reasons for retaining transaction data that override such requests.*
6.	Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures *This means organisations need to have strong website and server security, a data breach response process, data deletion policy and training for all employees so they understand how to handle data.*
7.	Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR *This means that organisations are expected to put into place comprehensive but proportionate governance structures to prove compliance with the GDPR to any Privacy regulator. These governance structures may include Data Protection policies, audits of systems and data flows, staff training, and Data Protection by Design where Privacy teams are an integral part of design of system build.*

The GDPR provides the following rights for individuals

Further demonstrating an organisation's responsibilities under GDPR

1.	The right to be informed	• The organisation has to provide 'fair processing information', typically through a privacy notice. • It emphasises the need for transparency over how you use personal data.
2.	The right of access	• Individuals have the right to access their personal data and supplementary information. • The right of access allows individuals to be aware of and verify the lawfulness of the processing.
3.	The right to rectification	• The GDPR gives individuals the right to have personal data rectified. • Personal data can be rectified if it is inaccurate or incomplete.
4.	The right to erase	• The right to erasure is also known as 'the right to be forgotten'. • The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5.	The right to restrict processing	• Individuals have a right to 'block' or suppress processing of personal data. • When processing is restricted, you are permitted to store the personal data, but not further process it. • You can retain just enough information about the individual to ensure that the restriction is respected in future.
6.	The right to data portability	• The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. • It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. • Some organisations in the UK already offer data portability through the 'MiData' and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. • It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.
7.	The right to object	Individuals have the right to object to: • Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); • Direct marketing (including profiling); and • Processing for purposes of scientific/historical research and statistics.
8.	Rights in relation to automated decision making and profiling	The GDPR has provisions on: • Automated individual decision-making (making a decision solely by automated means without any human involvement); • Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Source: ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Challenge & Opportunity for financial services

The GDPR aims to harmonize European member state privacy laws but will also introduce sweeping powers for regulators and, in turn, comprehensive enterprise risk and fines similar to those for breaches of anti-trust and competition law.

Not surprisingly, media and industry commentators are paying close attention, with inevitable countdowns to the May 25 deadline and conjecture about regulators making early examples to show their 'new teeth'. Over and above this chatter, there are five themes worth exploring for financial services.

1) Privacy and Data Protection: more than just security

Security alone will not demonstrate good privacy practice as per the earlier analogy of a house made of bullet proof, yet transparent, glass. In the modern era of user-centered ecommerce and connected business, security of data and systems as well as wider customer data privacy must be managed holistically.

The European Parliament has been clear that it will not settle for anything other than the highest standards of privacy protection. This is mirrored by guidance from the European Data Protection Supervisor (currently Art 29 Working Party) and local regulators such as the Information Commissioner's Office in the UK. Businesses should be investing in building out the Privacy Function within their organisation so Privacy can be integrated into all business activities. This will be crucial for maintaining customer trust when their enhanced rights come into effect in May.

2) At the compliance coalface

Compliance with the GDPR demands a step change in operation and process from May 25 2018, including:

i) Proactive proof of compliance: Organisations will need to establish and maintain evidence logs in readiness to submit to regulators in the event that a complaint is made against them. This replaces the current lighter touch process whereby only as and when regulators raised questions about compliance did businesses have to provide specific answers. Unless, in rare cases, they were audited by their regulator.

The evidence required going forward may include any ongoing reviews or quality assurance and updates to compliance measures, maintenance of breach registers, data flow maps to show where personal data are held and transferred, and accountability registers for risk owners so that individual business leaders within your organisations, responsible for processing personal data, can demonstrate compliance with the requirements by taking a 'privacy by design' approach. This may also include maintaining records of system design documents and privacy impact assessments that show why particular business processes were implemented surrounding the collection and use of customer data.

ii) Breaking old habits: The "'But we've always done it that way" excuse will not cut it under the GDPR.

Business needs to reassess every point of customer data capture and each use of that data to ensure the correct legal basis for processing those data. Simultaneously, e-marketing consent requirements look to become even harder under the proposed e-Privacy Regulations. These are recognised as no easy tasks, but are essential for compliance.

However, the greatest challenge may be education and awareness among those functions, such as sales and marketing, that need to adjust tried and tested strategies and plans to ensure compliance past May 25.

3) Special category data

Under the GDPR, biometric data will be classified as 'special category data' meaning privacy, identity and security will be critical to the next generation of data-driven businesses. Such businesses will inevitably make use of cutting edge biometrics technologies for user authentication, evolving the current use of by fingerprint, voice, facial recognition, and hand geometry.

Deeper behavioural traits including typing rhythm, walking gait and hand tremor pattern analysis are the bio-data points likely to be harnessed next. As is the power of computers to use 'liveness detection' algorithms to distinguish between photographs of faces and real people.

Where biometric data is to be collected, careful consideration must be given to the implications of a data breach where the very essence of an individual, their uniquely personal identifiers, are lost or in some way compromised.

4) Frictionless payments: A convenience vs security conundrum

The increasing adoption of biometrics as a default payment mechanism and the deeper penetration of digital identity technologies are paving the way for frictionless payments to become a full-blown reality.

However, as soon as a new payment or currency-based instrument evolves, so too does a form of fraud to exploit it. As Paysafe's Lost in Transaction research report found, the balance between frictionless payments and robust security measures is a delicate one. The convenience versus security conundrum will continue to challenge business leaders looking to capitalise on the anticipated lift in global revenues from $1.3 trillion in 2014 to $4.5 trillion in 2021*.

Building new mechanisms for electronic commerce can be complex. Business seeking to apply technologies in this space must look for platforms and tool kits with enough resilience to protect against a range of possible threats to security and privacy, from malicious hackers, organized cause-motivated hacktivists and rogue nations.

*Source: Statista

5) Levelling the playing field for SMBs

In most modern economies, small and medium-sized businesses (SMBs) now drive a substantial portion of revenues and governments are aligning both growth programmes and tax regimes to accommodate this economic shift. The implementation of the GDPR, e-Privacy Regulations and PSD2 Directive are intended to make trading easier for SMBs and to stimulate growth in this sector.

Being small is less of a disadvantage in today's digital world. Indeed, SMBs are often more agile and able to react in a more timely manner to data-derived insights than their larger counter parts.

SMBs are already starting to identify the payment processing world as the logical provider of a variety of data solutions, including real-time reports, payment information, inventory, employee management, social media and other useful marketing information.

Empowering SMBs with the opportunity to access consumers, mobile payments and data levels the playing field and increases their competitiveness against bigger organisations.

About Paysafe

At Paysafe, we are building the future in payments and ecommerce: an ever-evolving platform that meets the needs and expectations of tomorrow's businesses and consumers.
Having been at the centre of innovation in payments since 1996, we understand how to stay ahead of the curve. How to anticipate new customer needs. How to react to changes in regulation.

How to leverage new technologies. How to adapt and be agile. This is what defines us. That's why at Paysafe, you will see a portfolio and set of capabilities that is always growing. Never standing still, never complacent.

From cash to digital currency; from all-in-one processing to multi-currency consumer wallets and remittance; from order-ahead mobile apps to consumer credit solutions, our unique portfolio for merchants, partners, developers and consumers comprises industry-leading capabilities in payment processing, digital wallets and online cash solutions.

Paysafe