Executive summary

This white paper examines the relationship between two new regulations impacting on merchants and their third-party service providers in 2018, and brings into context the existing contractual obligations defining the minimum data security standards for storing, processing and transmitting payment card data.

Designed to be helpful to those responsible for payments compliance in both the public and private sectors, the paper shows that both regulations - the General Data Protection Regulation, becoming law in the UK through a single piece of legislation, the Data Protection Bill 2017, and the Payment Services Directive 2 (PSD2) brought into UK law via three pieces of legislation: The Payment Services Regulation 2017; The Payment Services and Systems and Electronic Money Regulation 2017; and The Financial Services (Payment Services) Regulation 2018 - collectively establish the legal frameworks to promote electronic commerce and secure third party data within those frameworks.

With signposting to relevant information sources and quotes from expert authorities, the paper draws parallels between what the new regulations seek to achieve and the steps already taken by the payment card schemes through the establishment of the Payment Card Industry Security Standards Council (PCI SSC) and the ecosystem promoting card data security and maintaining compliance to the Payment Card Industry Data Security Standard (PCI DSS).

The document also draws attention to how the UK’s drive to reduce costs of customer acquisition has differed from other EU member states and highlights that the attention given to providing the customer with the ability to self-serve has not been matched with an entity’s ability to secure access to that customer’s data.

Summary conclusion

After offering evidence of UK consumer attitudes to data security and data breach, the document concludes that personal data security will become increasingly valued by the customer and organisations who fail to position data security and compliance higher in their value proposition will become less attractive to their existing and prospective customers.
Foreword

The General Data Protection Regulation (GDPR) becomes legally enforceable on 25 May 2018. Described by the UK Data Commissioner and many industry commentators as a ‘game changer’, this regulation is creating a significant level of discussion across all industry verticals.

Having predominantly been in the domain of the legal, risk management and information security communities, data protection considerations are now impacting on business operations. This paper is positioned to help those involved in processing payments and outlines the data regulations impacting directly on the payments environment.

The content below covers the relationship between Payment Services Directive 2 (PSD2) which came into effect on 13 January 2018, the General Data Protection Regulation (GDPR), and the existing contractual legislation that covers payment card transactions - the Payment Card Industry Data Security Standard (PCI DSS). By providing an overview of the relationship between these regulations, the aim is that those directly supporting the payments process gain a better understanding of the compliance obligations impacting on corporate governance and the potential commercial impact if proper governance of data security and data processing is not maintained.
In summary: the new regulations and the payments industry data security standard

**General Data Protection Regulation (GDPR)**

GDPR sets out a common legal framework for governments, public authorities, businesses and consumers when interacting with each other within the European Economic Area (EEA) and applies equally to all entities trading with the EEA.

The text clarifies customers’ (data subjects) new rights and sets out the definitions of different data types, setting out the legal obligations of data controllers, data processors and data sub-processors when interacting with data subjects and with each other.

The regulation upholds the right to privacy as set out in the European Convention on Human Rights (ECHR) and brings these rights in line with the growth in social media and the use of 'big data'. Compliance with the regulation means that the way in which entities process data is more transparent to customers and imposes significant obligations on entities to keep personal data secure.

**Payment Services Directive 2 (PSD2)**

PSD2 sets out a common legal framework for businesses and consumers when making and receiving payments within the European Economic Area (EEA).

The text makes it clear that customers have a right to use what are termed Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) where the payment account is accessible online and where they have given their explicit consent. These changes reflect the market growth in e-commerce activities and use of internet and mobile payments, as well as the rise of new technological developments and a trend towards customers having relationships with multiple account providers. Compliance to PSD2 will make internet and mobile payments easier and help customers to manage their accounts and make better comparisons of deals between service providers.

**Payment Card Industry Security Standards Council (PCI SSC)**

PCI DSS sets out a common security framework for all entities when making and receiving card payments anywhere in the world.

The text forms part of the contractual relationship between the merchant and their acquiring bank and makes it clear how payment card data is to be secured. The text also applies to all other entities within the secure payments ecosystem, with the two exceptions being the payment card schemes (Mastercard, Visa, American Express, Discover, JCB) and telephony carriers (transmitting data end to end only). The PCI DSS has evolved to reflect the market growth in cyber-crime and the fraudulent use of payment cards to buy goods and services. Compliance to the standard makes payment card data more secure and reduces the risk of data breach.

All of which means that 2018 is going to be a year of significant change for all entities across the public and private sectors processing payments for EU persons within the European Economic Area (EEA).
The GDPR in context

The GDPR represents the most significant change in the payments environment in terms of risk to merchants (data controllers) and entities supporting data processing (data processors and sub-processors).

Made up of 173 recitals and 11 chapters containing 99 articles, the GDPR places great emphasis on transparency, which means an obligation on merchants and processors to share information with their customers. In real terms this is us as individual data subjects. The regulation also transfers the ownership of data back to the customer, the data subjects.

In brief, after setting out General Provisions in Chapter I and Principles in Chapter II, the regulation then describes our rights (as data subjects), some of which already exist under the previous EU legislation (which underpinned the UK’s current Data Protection Act), others of which are new. Collectively, these new entitlements, enforceable in law from 25 May 2018, entitle us as data subjects to seek ‘remedies’ which are laid out much later in the document, in Chapter VIII (Remedies, Liability & Penalties).

Within Chapter VIII, under Article 79, we have the right to effective judicial remedy against the controller or processor and, under Article 82, we have the right to compensation. That compensation, whilst likely to be both proportionate and dissuasive, is unlimited. This new emphasis on putting the data subject first is significant enough in terms of risk.

However, what makes GDPR the ‘game changer’ that many describe, are three more fundamental changes:

The first is that Chapter VIII entitles the data subject to seek ‘remedies’ from both the data controller and the data processor, as well as the data processor’s entire supply chain supporting the processing of data. That means a notable change in risk profile for all data processors and the sub-processors who support them in processing transactions, which in turn means that all contracts between all parties have to be reviewed in the context of this change.

Secondly, there are specific obligations on the data controller and the data processor in Chapter IV to document all data processing to the extent that those parties are guilty until they can provide evidence that they have met those obligations within the regulation.

Finally, again under Chapter IV, Article 28 puts two obligations on controllers and processors in that it states “where processing is carried out on behalf of the controller, 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.”

This not only means that the data processor has direct exposure to fines directly from the ICO and direct exposure to data subjects’ rights, but also an obligation to ensure our data is secure by only trading with entities that can provide sufficient guarantees to meet the requirements of the Regulation.

That not being enough to keep the marketing community on their toes, Article 28.2 states that “the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.”

Thus, as well as having a direct impact on the ‘change control’ process between data controller and data processor, and between data processor and data sub-processor, Article 28 introduces the idea of a ‘chain of compliance’ where the data controller’s ongoing compliance is dependent on the compliance of their supporting data processors and sub-processors. This approach is in common with that taken by payment card schemes within the PCI DSS, where within Requirement 12, the PCI DSS seeks to ensure that everyone involved in the supply chain impacting on the security of the card scheme’s data, such as merchant and third party service providers, are obliged to operate under the same security requirements and security controls.
A framework to process transactions whilst protecting third party data

It’s apparent from the above summaries of the regulations that GDPR, PSD2 and the PCI DSS are all written to support transactions between participating parties. However, each prioritises different parties within the transaction process.

GDPR puts the rights of the data subjects/consumers above all others, legally obliging both data controllers and data processors to put the interests of the data subject above their own. PSD2 is wholly dependent on the GDPR to firmly establish the legal rights of the data subject and the legal obligations of the data controller and processor in order to support the framework it sets to secure transactions between merchants and their customers. Conversely, the PCI DSS is almost devoid of text to do with the data subject and is written specifically to protect the payment card data through a contracting structure (either directly with merchants in the US or via acquiring banks elsewhere) owned by the card scheme and puts contractual obligations on merchants and their supply chain, to keep that data secure.

As a general observation, it’s interesting that of the 99 articles and 173 recitals within the GDPR, the vast majority of the 88 pages are dedicated to what the data subjects’ legal rights are, and what the legal obligations are of other supporting parties, the data controller and the data processor. Only 1 article (Article 32 - Security of Processing) and 2 recitals (78 and 83) provide direct instruction on ‘how’ data is to be secured.

That is in direct contrast to the PCI DSS, which not only says what, but has grown in size significantly over its lifetime to help participating parties understand how third party data should be secured. Whilst starting out as an amalgamation of the Visa™, Mastercard™ and American Express™ security programmes and just 17 pages when first published, the document is now in its sixth iteration and is a hefty 139 pages. As the security landscape has changed, so has the PCI DSS evolved in an endeavour to keep pace with those changes, whilst still maintaining the familiar structure within its original 12 requirements. What has basically changed in the PCI DSS is the number of pages dedicated to providing assessment and validation guidance, and the number of additional pages providing clarifications for all participating parties. What has also evolved alongside the PCI DSS document itself is a structured support infrastructure driven by the PCI Standards Security Council (PCI SSC) to drive consistency of understanding of the DSS and consistency of compliance certification through education and growing professional development programmes. For those directly involved with securing the payments process, The PCI SSC have been keen to promote user participation through their Participating Organisation program, Task Forces and Special Interest Groups (SIGs) that support the development of PCI DSS globally.

As a mature security framework, the PCI DSS will never have the same supporting infrastructure as the GDPR and PSD2 which are both supported by EU and national government data protection, as well as financial services authorities. And whilst that, and the levels of penalties for non-compliance might, by some, put the PCI DSS down the pecking order in terms of business priorities, what the PCI DSS offers is a mature framework on how to secure third party data.
The relevance of PCI DSS as a security framework for third party data

Under the GDPR (Article 25), entities have a general obligation to implement technical and organisational measures to show they have considered and integrated data protection into their processing activities. Recital 78 goes further and says, "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features."

Recital 83 is more specific about ‘how’, saying, “In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.”

Where to start with ensuring future data compliance

Whilst there is a significant part of the GDPR that references data minimisation, it’s not yet clear how the EU’s Article 29 Working Party is going to support the national authorities in providing an answer to ‘how’ entities are going to transition to comply with the GDPR by implementing ‘organisational measures’ as well as provide more detail on ‘technical measures’. Where most entities are likely to require help is in understanding the exact requirements of providing data security by ‘design and default’, as defined in Article 25, and written guidance on this would be useful. The Information Commissioner’s Office (ICO) website, however, offers early guidance on considerations for ‘privacy by design’ and indeed cites seven principles adopted in Canada as a good point of reference.

However supportive the current UK and Canadian guidance is, the PCI DSS provides a sound starting point for any organisation when considering ‘how’ to implement and maintain data security by design and default. To provide some context to how entities should approach securing third party data, the PCI SSC has taken a specific approach in framing their advice to comply with the DSS. Troy Leach (CTO PCI Standards Security Council) said in support of new PCI DSS scoping guidelines published in December 2016:

“This guidance, along with the card schemes’ acceptance in May 2016 that the acquiring community can now certify a merchant’s compliance on a channel by channel basis (face to face, e-comm and MOTO), equips entities with a much greater capacity to reduce the burden of payments compliance and focus their resources more exclusively on their wider personal data compliance obligations.

Troy Leach’s reference to “limit exposure of payment data” is far more easily achieved today (2018) than it was two years ago when the news of the GDPR’s adoption was first published on the European Parliament website. Secure ‘attended’ and ‘unattended’ solutions in the face to face channel are well supported, as are web redirection and tokenisation solutions to take e-commerce payments out of scope and thus reduce the time, cost and effort taken up in the compliance management and reporting process.

The PCI SSC have supported this by publishing guidance in their Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation from May 2017 and intend to do the same with MOTO payments following outputs from the new Secure Telephone Payments Data SIG announced in December 2017.

The compliance process for PCI DSS is now mature, with a global uniformity for self-assessment, external audit, compliance certification and forensic investigation.

That is not to say that interpretation amongst merchants on how to comply with the PCI DSS is consistent on a global basis - it is not. Nor is it to say that the PCI DSS certification audit across the globe is consistent. To support the ongoing security of the card schemes, payment card data requires consistent education and the guidance support of the merchants, the payment service providers and other third parties supporting the payments ecosystem (including issuers and acquirers), the QSA community supporting certification and the technology vendors supporting the payments process.

For the PCI Standards Security Council, supporting the education and guidance programmes is an ongoing exercise. Centered on a well published theme of getting risk off the table, taking payment card data out of the operational environment, 2018 will see the publication of updated guidance on securing telephone payment data, which was last issued in 2011 under version 2 of the standard. These new guidelines will focus on educating the acquirer and QSA communities as much as merchants and payment gateways. They will offer the secure payments community the latest insights on how to minimise the risk of data compromise in the telephone environment and the impact of organised crime on those employees listening to spoken payment card data over the telephone.
Protecting against regulatory breach

Guided by the EU’s Article 29 Working Party (made up of all national authorities) and by the national authorities themselves, public and private sector managers across Europe are preparing for this game-changing legislation which will impact on every area of data processing, including the processing of payments.

GDPR incentivises entities to make the transition in three ways: firstly by making it a legal obligation; secondly by including text (detailed in Article 83) setting out the level of fines and for what type of infringement those fines become enforceable; and thirdly by directing national authorities towards imposing fines (detailed in Article 84) by stating that “penalties shall be effective, proportionate and dissuasive”. This, put very simply, means that the ICO will not use 25 May 2018 as the start of a ‘grace’ period, but as UK Information Commissioner (Elizabeth Denham) put it, “the beginning of a journey.”

Additional challenges for UK entities

For UK entities, GDPR transition to a data processing regime governed by GDPR under the new Data Protection Bill 2017 (replacing the current DPA) will be harder than for entities elsewhere in Europe. This is because of the innovative ways in which UK entities have deployed technologies and business processes over the last twenty-five years or so to reduce the cost of managing their customers, both in terms of acquisition and service.

This divergence could be put down to the successful lobbying of trade bodies (Institute of Direct Marketing and the Direct Marketing Association – now converged as the UK DMA) to self-regulate as opposed to other EU member states, such as Germany and the Netherlands taking a state driven regulatory approach with a greater emphasis on the European Convention on Human Rights and the privacy rights of individual data subjects.

The relevance of the EU Privacy and Electronic Communication Regulation (PECR) to GDPR

Neither is it just the GDPR that entities need to consider. The new legal obligations on processors and controllers, covering the use of electronic communication in marketing under the EU Privacy and Electronic Communication Regulation (PECR), also applies. The PECR directly compliments and sits alongside the GDPR and an updated version was originally due to be passed into EU law on the same date as the GDPR. Due to delays, this will not be the case.

This means that the lines between compliance and non-compliance will need careful consideration until both sit in law together. As with GDPR, it’s important to use the ICO themselves as the primary source of information supporting a UK entities compliance strategy. The ICO website includes helpful guides to PECR and GDPR and offers its readers a pragmatic and comprehensive approach to meeting these new data regulations.

How the ICO plans to enforce the requirements

What is also worth establishing by visiting the ICO website, is the approach to the plan to regulate ‘the journey’ and how, under Elizabeth Denham, the ICO have interpreted the current Data Protection Act. A good example of this is the ICO’s approach to the charity sector in 2017. More evidence of this ‘firm but fair’ approach can be seen on the ICO’s website offering guidance on a sector-specific basis and supporting that with easy to follow checklists against each aspect of the Regulation and in a more informal way, by addressing entities’ concerns and misunderstandings directly through the ICO’s blog with contributions from Elizabeth Denham herself under the heading of ‘dispelling common myths’.

The opportunity to deliver a competitive edge in the age of customer choice

Recent ICO blogs go to great lengths to make clear that 25 May is not a Y2K type event, but the beginning of a journey. This can be reasonably understood to mean that UK entities are being directed towards mapping out that journey, to demonstrate to the ICO that they are making personal data security and legal compliance a cornerstone of their approach and, in so doing, are creating a ‘defendable position’ against regulatory fines.

This message is reinforced in Elizabeth Denham’s video address to UK Board Rooms in June 2017 where she states: “Get data protection right, and you can see a real business benefit...the pay-off here is not just in better legal compliance, but in competitive edge, and whether that’s in terms of attracting more customers or addressing more pressing public policy needs, I believe there is a real opportunity here for organisations to present themselves on the basis of how they respect the privacy and dignity of individuals.”

It’s clear that the content of the address deliberately directs UK private sector organisations towards the more recognisable incentive of ‘growth’ and the public sector towards ‘service delivery’. It is also evident our Information Commissioner envisages UK consumers will begin to make choices based on a new type of trust, a trust driven by an entities’ ability to keep data secure, rather than just delivering a reliable product or service, and doing that consistently over time.
How important is data protection to the consumer?

To benchmark a potential shift in how the UK public makes product and service consumption choices, research was undertaken by consultancy firm Compliance3 in 2016/17. This research recorded UK consumer responses to sets of questions about payment and personal data security pre- and post- data breach. The research consisted of 8 ‘pulses’ of 1,000 responses to 3 questions, each with multiple choice answers. Some results of note include;

- Whilst over 60% of respondents felt confident that data was being stored safely and securely, 80% of respondees stated that companies who did not do enough to protect payment card data should be named and shamed.
- At the point of data breach news being communicated, the first thing that 50% of male and 60% of female respondees said they would do is phone up the brand, which is a clear pointer towards response planning.
- 40% of those surveyed believed the brand should contact them personally in the event of a data breach but 75% stated that all customers should be informed if payment card data was compromised.
- In terms of anticipated impact of data breach on the brand, the power of social media was clear. 70% of those responding stated that they would tell close friends and relatives with 40% telling everyone they knew.
- In terms of post breach purchasing behavior, 40% stated that they would not buy from that brand again.
- Over half of the respondees, representative of the UK population, stated that they would be happy to receive a compensation package worth between £20 and £100.

This insight into data access, transparency of processing and compensation ahead of consumers new rights should help in the prioritisation of resource allocation to support GDPR transition and in decision making when looking to position data security and compliance as a point of difference in their brand values.

What does the future hold?

It’s certainly an interesting question. It’s our understanding, following conversations with the ICO, numerous reputable legal firms, in-house legal counsel and a QC specializing in fraud cases, that no changes are expected in the core legislation over the foreseeable future. Just as the twelve requirements of the PCI DSS have remained core to the Standard, so the core principles of both PSD2 and GDPR (soon to be supported by PECR) are likely to remain relatively unchanged.

The need for additional expertise in an evolving payment landscape

Considering PSD2 first, the new legal framework will no doubt drive the API-led economy that so many have talked about in the press which offers the incumbent players within the existing secure payments ecosystem unprecedented opportunities to redefine their offers. As existing and new players define their strategies, the payment landscape will continue to evolve.

Acquirers will have to build new expertise to expand their payment capability and remain relevant with merchants. Issuers will need to review their products and propositions, moving away from traditional products and schemes. And card network operators still have the opportunity to play a central role in the payment lifecycle, so long as they support their clients in the digital evolution. While these scenarios can be predicted with some certainty, there are a number of areas where only time will define the specifics of the compliance obligations all participants find themselves in.

These are likely to include security and authentication mechanisms as well as the emergence of a risk management framework needed to address barriers in the development and uptake of these new services.

These will both have a significant impact on whether PSD2 successfully achieves its goal of providing a workable European alternative to processing payments using payment cards. What the card schemes have as their ‘trump card’ is the established ‘chargeback’ and accountability process that protects the consumer. Whilst some areas of liability have been defined within the text, it remains to be seen if EU consumers will be convinced to move away from using payment cards and if merchants, acquirers and issuers continue to support the revenue streams and profits of the predominantly US based payment card schemes.

As discussed earlier in this paper, the PCI DSS provides a sound reference, around which entities can begin to plan their approach to securing third party data, in the absence of any guidance within GDPR the PCI DSS is relevant to any entity, irrespective of whether or not that entity stores, processes or transmits payment card data. The PCI SSC continues to look to extend their reach with the introduction of new standards to support the secure payments ecosystem with the new standard launched in January for software-based PIN entry on commercial off-the-shelf devices (COTS) such as smartphones and tablets, being a good example. The speed and rate at which these new standards will be adopted by entities processing payment cards is uncertain, and will very much be dependent on the acquiring banks who, in the UK and Europe, hold the commercial relationship with the merchant.
Whatever payment methods EU consumers choose to use in the future, it’s clear from the first tranche of research shared above, that consumers are aware of data security and care about their data privacy. How quickly ‘awareness and care’ are seen to translate into ‘choice and selection’ is not yet clear, and future research tracking the thoughts and preferences of data subjects will be shared in future papers.

**Reprioritising customer data security**

What is much more recognisable is that for the last twenty-five years, whilst organisations across the world have been competing on service, successfully putting the customer at the centre of their operations and using technology to drive ‘self-service’ whilst placing data and data processing within the customers’ own reach, we have seen a parallel growth in cyber-crime.

The impact on the data subject themselves is picked up in the Compliance3 research showing the potential impact of data breach on future purchasing behaviors. What is also evident from the increasing levels of reported cyber-crime and data compromise is that, in general terms, entities have prioritised customer acquisition, retention activity and reducing the costs of those activities over the security of that customer’s data.

It’s no surprise then that the regulation of entities is now focused on this new paradigm, of data processing being the basis on which human beings interact with each other and with which they consume products and services. Commercially and socially, data is now king, and data regulation is beginning to recognise this, forcing entities to create more balance between reducing their costs of customer acquisition and retention, and data security.

In the words of Elizabeth Denham “I want organisations to think to themselves: ‘we base our online user experience around what consumers want. We shape our products and services around what consumers want. We need to shape our data protection approach around what consumers expect’.”

“**I want organisations to think to themselves… ‘We need to shape our data protection approach around what consumers expect’.”**

Elizabeth Denham, UK Information Commissioner

---

**About Pay360 by Capita**

Pay360 by Capita is a leading independent UK payment service provider, offering a range of global, modular payment, compliance and fraud solutions. Pay360’s flexible range of card and cash payment solutions make it easier for customers to pay however they choose, whilst our advanced fraud management solution can be applied to anti-money laundering, KYC and identity verification. Pay360 is uniquely positioned to provide compliance expertise, helping organisations improve efficiency whilst meeting their compliance obligations under GDPR and PCI DSS.

**Contact Pay360 by Capita**

(0)333 313 7160
pay360digitalsales@capita.co.uk
www.pay360.com

**Keep in touch**

Twitter: @Pay360byCapita
LinkedIn: Pay360 by Capita
Facebook: /Pay360byCapita

---

**About the author**

John Greenwood is Director of Thought Leadership at Compliance3 and supports the COMPLY proposition for Capita Pay360 that helps merchants reduce the time, cost and effort in meeting their PCI DSS compliance requirements. He has spent over 25 years in the customer contact centre space helping leading brands interact with their customers to reduce cost and improve service.

john@compliance3.com

---

**About Compliance3**

Compliance3 is a technology agnostic professional services firm with a heritage in delivering large change projects in the contact centre environment. They help governing bodies and acquiring banks define and support compliance guidelines whilst at the same time help public as well as private sector organisations meet their payments and personal data security obligations, reducing the time, cost and effort in achieving and maintaining compliance.

www.compliance3.com