
# GDPR AND PSD2:

## ARE YOUR APPS READY?

MAY, 2018



verimatrix
DRIVING TRUST

# TABLE OF CONTENTS

Executive Summary

# ARE YOUR APPS READY FOR GDPR AND PSD2?

European Union lawmakers are having a global impact on how mobile applications are viewed. No longer can they be viewed solely as a customer engagement tool where the only thing that counts is a great User Experience. Protecting the users of those applications has become equally important.

All companies now need to ask themselves: are our Apps GDPR ready? **Most organisations are aware of the extra requirements to protect personal data that GDPR put on them; but most have also forgotten that their mobile applications put that data exactly where GDPR does not want it to be: in the clear outside of the IT firewalls.**

While GDPR is generic legislation that affects everyone, PSD2 is focused on the payments industry. It is designed to shake up the payments ecosystem – opening up services to new players.

There is no need to be scared of the new regulations. The most important thing is to be aware of the legalisation and understand its applicability to your organisation.

As always with mobile, there is a great opportunity. **Those organisations that truly understand mobile and use it to their advantage - rather than just reacting to new requirements - will be the ones that win.**

With the right approaches not only can the new requirements be met; but the user experience can actually be improved. Turning the necessity to adapt into an opportunity to improve user convenience and ultimately drive adoption of services.

# INTRODUCTION

**Two major new regulations are driving massive changes to how organisations manage their customers' data.**

The first of these new regulations is the **General Data Protection Regulation (GDPR)**[1]. This affects all organisations that process or store personal data of EU citizens.

The second regulation is **2nd Payment Services Directive (PSD2)**[2]. This focuses on opening up banking services to non-banks and securing online payments with Strong Customer Authentication. It therefore directly impacts on banks and fintechs, but opens up new business opportunities wider than that.

While coming from the European Union (EU), they are having an impact globally. Partly as they affect any organisation that is doing business in the EU; but also because they are influencing governments and regulators around the world.

It is worth pointing out that the UK is committed to implementing both regulations despite its intent to leave the EU.

Much of the discussion around GDPR and PSD2 has forgotten that mobile applications process personal data and interact with payment services. This brings these apps in to the regulatory scope. **Organisations cannot afford to forget this. This paper not only discusses the risks to avoid but also highlights the advantages that can be gained by remembering mobile as part of your wider GDPR and PSD2 strategy.**

1 https://gdpr.eu/

2 https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

# GENERAL DATA PROTECTION REGULATION (GDPR)

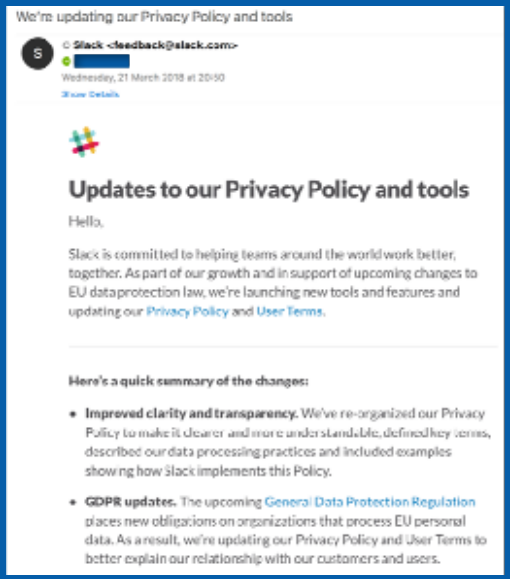
## Principles

GDPR replaces the Data Protection Directive 95/46/EC. It aims to harmonise data privacy laws across Europe while protecting and empowering EU citizens with new rights. This will reshape the way organisations across the region approach data privacy.

In effect, EU citizens will own any information about themselves. That data is only lent to organisations. These organisations then have a duty of care to keep that data safe.

Every organisation that handles EU citizens' data is affected. This means that the regulations will affect non-EU based organisations, as well as EU based ones.

The Enforcement date is the 25th of May 2018 - at which time those organisations not complying may face heavy fines.


We're updating our Privacy Policy and tools

Slack <feedback@slack.com>

Wednesday, 21 March 2018 at 20:50

**Updates to our Privacy Policy and tools**

Hello,

Slack is committed to helping teams around the world work better, together. As part of our growth and in support of upcoming changes to EU data protection law, we're launching new tools and features and updating our Privacy Policy and User Terms.

**Here's a quick summary of the changes:**

- **Improved clarity and transparency.** We've re-organized our Privacy Policy to make it clearer and more understandable, defined key terms, described our data processing practices and included examples showing how Slack implements this Policy.
- **GDPR updates.** The upcoming General Data Protection Regulation places new obligations on organizations that process EU personal data. As a result, we're updating our Privacy Policy and User Terms to better explain our relationship with our customers and users.

*All EU citizens will be getting lots of emails like this one from Slack*

# Key Points

The most important point to realise is that any data that can directly or indirectly identify an individual is in the regulatory scope. Such personal data must be protected wherever it is stored or processed.

It is also worth noting is that protection of any personal data must be taken seriously by all organisations – it cannot be an afterthought or ignored. There is a requirement for organisations to build in *"privacy by design"* and to use *"state of the art"* security.

**Beyond these key points, GDPR gives EU citizens some important rights :**

**Right to privacy:**

Personal data cannot be shared publicly or with other organisations without the user's / customer's consent. This means that personal data must be protected to stop unintended sharing; and mechanisms put in place to collect consent for intended sharing.

**Right to be forgotten:**

If an EU citizen asks an organisation to delete all their personal data, the organisation must response and may have to comply.

**Right of access and portability:**

EU citizens have a right to know exactly what data an organisation is keeping on them; and in certain circumstances they can access that information in such a way that it is easily passed onto another organisation.

**Right of breach notification:**

If an organisation fails to protect data and it falls into 3rd party hands without consent, the organisation that was breached has to inform everyone impacted.

GDPR comes with enforcement powers designed to make sure it is better for business to respect those rights. For organisations that do not, fines of up to €20m or 4% of revenue (whichever is higher) await.

# Mobile Specifics

Mobile devices are about convenient and easy access to services and data. That means that they display, process and store lots of personal data. Remember, any data that can directly or indirectly identify an individual is in the regulatory scope, so personal data on mobile devices needs to be protected at rest, in transit and during use.

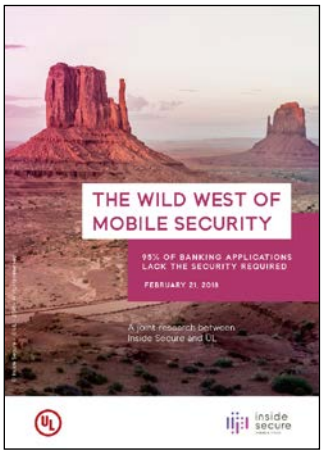
The analysis of Mobile Banking apps carried out for Verimatrix and UL's "Wild West" research[3] highlighted that **most organisations are unaware of the risk they are putting themselves under.**

The apps tested were often found to rely on the limited protection that come from the Android and iOS operating systems. Over the years, these protections have been demonstrated to be easily broken down or circumvented.

It was also found that most cryptographic operations simply used operating system provided functionality. Any cryptographic implementation is only secure as long as the cryptographic key is kept secret. Using operating system functions provides attackers with an easy attack vector to retrieve the key. Therefore, using algorithms packaged with the operating systems is not state of the art.

This means that **organisations should be protecting their applications with strong Code Protection technologies that resist attempts to reverse engineer or modify code** (sometimes known as RASP[4]). Whitebox cryptography provides a proven technology to keep those cryptographic keys safe even in open and insecure environments like mobile phones. Combined, these technologies and techniques would be considered "state of the art".

Despite the points made above, mobile should not be viewed as a problem that needs to be solved. In fact it is part of the solution. Ensuring privacy means ensuring that only authorised people have access to data. Replacing legacy username-and-password systems with modern Strong Customer Authentication (SCA) approaches not only increases security but also improves the customer journey.




Today "state of the art" SCA implementations are designed around the mobile device. This brings that all-important convenience. It also provides an additional authentication factor and so increases security.

Going further, SCA also secures the Right to Access and Portability, and Right to be Forgotten, by enabling service providers to easily request consent from the right user.

[3] Read the White Paper on : https://www.verimatrix.com/resources

[4] RASP – Runtime Application Security Protection – one of a number of acronyms for Code and Application protection

# 2ND PAYMENT SERVICES DIRECTIVE (PSD2)

## Principles

Concerns that the payment industry is being dominated by a handful of big players, led to the EU introducing the second Payment Services Directive. The directive's purpose was to:

- **Increase competition and participation in the payments industry from non-banks,**

- **Provide a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users.**

**Open Banking**

instructs banks to open their services via APIs.

**Strong Customer Authentication**

for financial transactions and Open Banking access

While the directive came into force on the 13th January 2018, that is only part of the story. The Regulatory Technical Standard (RTS) on Strong Customer Authentication and Common and Secure open standards of Communication ("Open Banking")[5] became official on the 13th March, 2018. Service Providers have until 14th, September 2019 to comply with the RTS.

[5] http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

# Key Points

## Open Banking

The Open Banking provisions of PSD2 are intended to shake up the relatively static banking and in payment sectors. The directive makes banks provide access to their services to non-banks (and competitor banks). The entities accessing these services are known as Third Party Providers (TPPs). The TPPs are then able to build banking-like consumer facing services that build on the existing banking infrastructure.

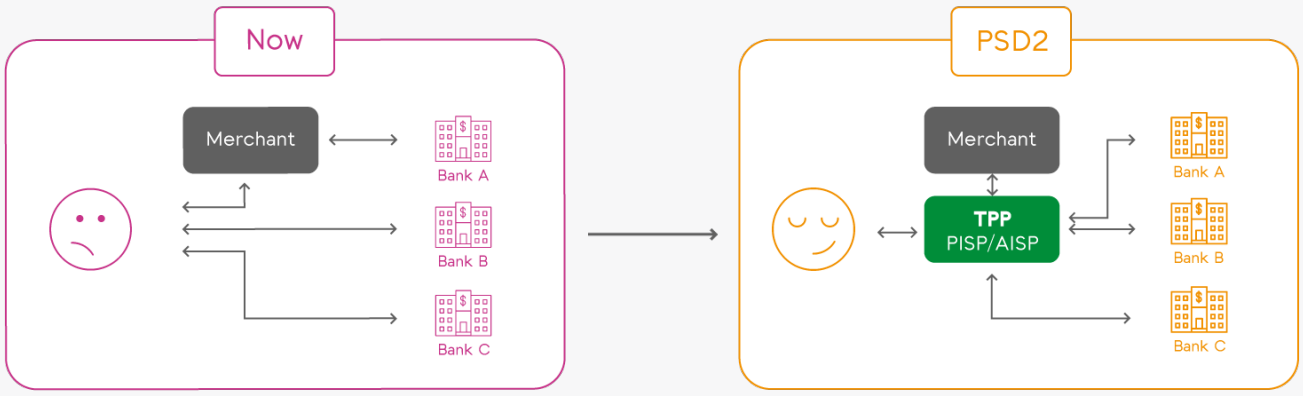
As well as access to services, the directive also breaks down the banks' monopoly on their users' data. The directive requires banks to implement APIs, through which the TPPs can access the banking data. This legitimises services like account aggregation that previously had to rely in screen-scraping.

Two categories of Third Party Providers (TPPs) are defined:

- **Payment Initiation Service Providers (PISP)** - This allows third party companies to initiate payment on behalf of a consumer without them having to visit their online bank's portal. PISPs offer consumers flexibility when it comes to payment.

- **Account Information Service Providers (AISP)** - This will allow third party companies to access a consumer's bank, as well as display information relating to their account. For example, this could allow a consumer to aggregate information from multiple accounts in a single application giving them an overview of their financial situation.

**Open Banking : changing the way we transact**




Banks expose their customer payment and account data, with customer consent, to Third party Payment Providers (TPPs) via APIs.

Figure 1 - PSD2 changing ecosystem

PSD2 turns all companies who wish to participate in Open Banking into regulated Entities. This brings the TPPs under Banking Regulators' jurisdiction. This means they will be under the legislative powers of Central Banks, etc. This is a significant change for Payment Processors, Merchants and other "intermediaries" who have never had to comply with such requirements.

At a high level, the requirement for open access to bank accounts appears to conflict with GDPR privacy requirements – GDPR requires increased attention to maintaining data privacy, whereas PSD2 encourages data sharing. In fact, some banks are using GDPR as a defence/excuse for not implementing PSD2. Anecdotal evidence is that the European Central Bank is taking a very dim view of this.

The reality is that there is not a conflict. The GDPR requirement is that consent is given before sharing of data, not that data cannot be shared. This aligns with PSD2.

## Strong Customer Authentication

As with GDPR, Strong Customer Authentication is a key element when complying with PSD2. Discussed above was the requirement for consent when sharing data through Open Banking. PSD2 also strengthens the requirement for identity checks for transactions (e.g. 3D Secure for card payments).

As a general rule, SCA is required whenever accessing a payment account or making a payment - but that is not the full story (see box outs). There is also an allowance for risk management to be used for slicker user journeys; provided the fraud levels can be demonstrated using Transaction Risk Analysis (TRA) as lower than:

- When 13 bps (1.3%) for a transaction under €100;
- When 6 bps for a transaction under €250;
- When payer 1 bps for a transaction under €500 before a challenge is required.

PSD2 is clear about what is required for an authorisation to be classed as "strong".

### WHEN IS SCA REQUIRED?

- When payer accesses their payment account online;
- When payer initiates an electronic payment transaction;
- When payer carries out any action through a remote channel which may imply a risk of payment fraud.

The **first consideration is that for the Strong Customer Authentication, at least two out of these three factors are required: something you *know* and/or *have* and/or are. Something you know could be a PIN or password; something you have could be a mobile phone or credit card; and something you are could be a biometric.** There needs to be independence of the factors so that a breach of one of the factors does not compromise the reliability of the others.

Secondly, **the authentication needs to generate an authentication code that is tied to the transaction.** This code needs to be either a one-time code or a signature, and it cannot be derived or forged. Moreover, it should not disclose the authentication elements. The function of the authentication code is to provide non-repudiation, i.e. a proof that a transaction was properly authenticated.

Thirdly, **the process has to ensure confidentiality and integrity of credentials.** This includes performing the authentication over secure communication channels and protecting it against manipulation – particularly important if a multi-purpose device (such as a mobile phone) is used in the authentication process.

Note, the encryption techniques and flows used in the process must be fully documented. There needs to be evidence that the implementation complies with the requirements.

## WHEN IS SCA NOT REQUIRED?

- Accessing account balance or transaction data after the first use or within 90 days of previous SCA;
- Contactless payments of less than 50 EUR, or 5 consecutive payments cumulative < 150 EUR since SCA;
- Unattended transport or parking payment terminals;
- Trusted beneficiaries and recurring transactions;
- Payments to self;
- Low value transactions of less than €30, or 5 consecutive payments cumulative less than €100 since last SCA;
- Transaction Risk Analysis based demonstrates risk is below defined thresholds.

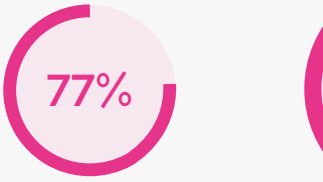
Finally, **the authentication should be protected from "lost and stolen" attacks.** This means it shall be blocked if authentication fails 5 times in a row, either temporarily or permanently; and the authentication is valid for a maximum of 5 minutes, only.

SCA on its own is not enough for PSD2. It is important to monitor the effectiveness of the access controls. As such PSD2 includes requirements to keep an audit trail including:

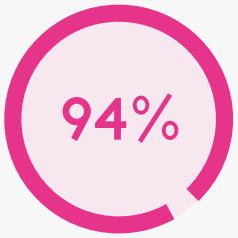
- List of compromised or stolen authentication elements;
- Amount of each payment transaction;
- Known fraud scenarios;
- Signs of malware infection in any authentication session.

Transaction Risk Analysis was mentioned above. It is an opportunity for the SCA requirements to be relaxed slightly as PSD2 provides some scope for trading SCA against risk – if the risk can be demonstrated as being low. If using this approach, monitoring must be in place to capture and run real-time risk analysis against:

- Payers previous spending and behaviourial patterns
- Payers payment transaction history;
- Location of the payer (abnormal or high risk);
- A log of the use of the access device.

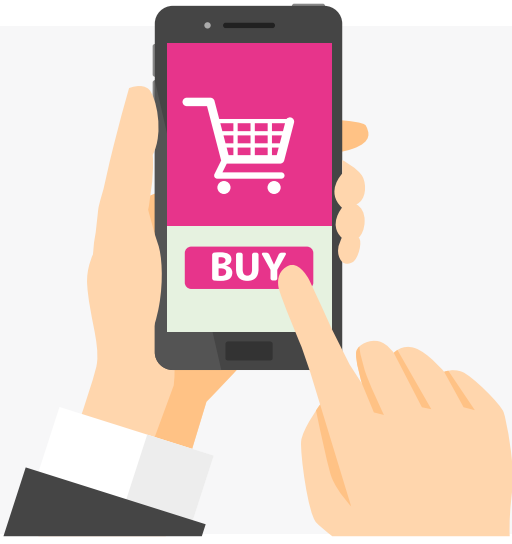



of Europeans use mobile banking[6]




of consumers say that new payment services must be as secure as existing ones


of people would not trust a 3rd party provider as much as a bank[7]




[6] https://www.visaeurope.com/newsroom/news/mobile-money-takes-off-as-77-of-europeans-use-their-phones-to-bank-and-make-everyday-payments

[7] Consumers' initial reactions to new services enabled by PSD2, Accenture Payments

# Mobile Specifics

Mobile devices have the characteristics required to meet the Strong Customer Authentication requirements for PSD2: they are flexible, personal and able to capture authentication. Plus they provide convenient means to implement the requirements.

While the best SCA user experiences are on mobile, care does need to be taken to mitigate the risk of a multi-purpose device being compromised. This mitigation must include use of separated secure execution environments through the application installed to ensure the application or device has not been altered. One approach that meets this requirement is to use strong and proven Code Protection and Whitebox technologies.

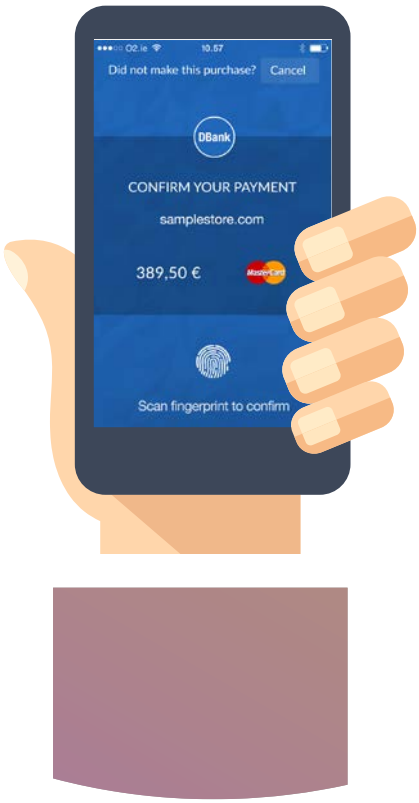



Figure 2 - Mobile can provide a rich SCA experience

PSD2 requires that the authentication is tied to a particular transaction (though batch and repeat payments are allowed). The payer must be made aware of the amount and the payee and the authentication process must generate a unique authentication code that is specific to the amount and the payee.

A PSD2 application (perhaps integrated into a mobile banking application) is a great way of achieving this. When authorisation is required, a message can be sent to the application containing secured details of the transaction. These details can be displayed to the user and authorisation requested. The mobile device itself can be the "something I have" factor with the device used to capture a second factor. This creates a very slick but also secure user experience.

The mobile is also a powerful computing device. Using this computation power to digitally sign the transaction provides the non-repudiation and audit trail required by PSD2.

# CONCLUSION

There is no need to be scared of the new regulations. The most important thing is to be aware of the legalisation and to understand where it is applicable to your organisation.

With the right approaches not only can the increased security requirements be met; but the user experience can actually be improved. Turning the necessity to adapt to new regulations into an opportunity to improve user convenience and ultimately drive adoption of services.

## WHERE DOES VERIMATRIX COME IN?

• **Code Protection Tool:** ensure that applications implementing Strong Authentication or managing personal data remain secure;

• **Whitebox Tool:** State of the art protection for personal data as required by GDPR;

• **Strong Authentication Solution:** Perfectly meets PSD2's strong customer authentication requirements.

• **Monitoring:** No-code integration to security monitoring provides real-time insights into the risk profile of your Android and iOS applications.

# About Verimatrix

Verimatrix (Euronext Paris – VMX) is a global provider of security and analytics solutions that protect devices, services and applications across multiple markets. Many of the world's largest service providers and leading innovators trust Verimatrix to protect systems that people depend on every day for mobile apps, entertainment, banking, healthcare, communications and transportation. Verimatrix offers easy-to-use software solutions, cloud services and silicon IP that provide unparalleled security and business intelligence.

Proud to empower and protect its customers for more than two decades, Verimatrix serves IoT software developers, device makers, semiconductor manufacturers, service providers and content distributors.

For more information, visit www.verimatrix.com.


verimatrix
DRIVING TRUST