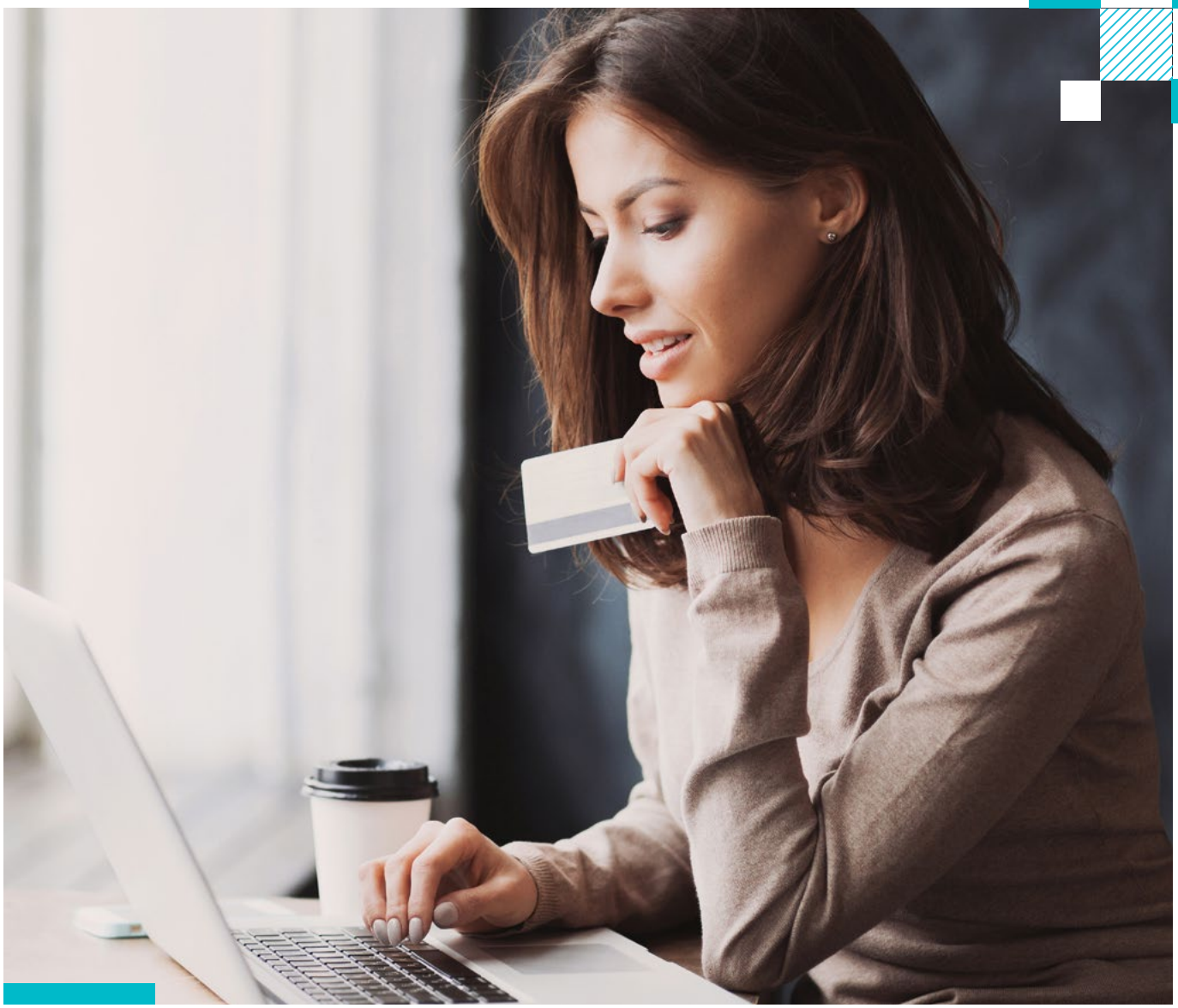
ingenico
ePayments

A Merchant's View: The Complexity of GDPR Unraveled in the World of Payments

Guidance For Non-EU Based Merchants And Most Commonly Asked Questions



INTRODUCTION

Beyond EU borders, most companies have now heard of the European General Data Protection Regulation (GDPR). It came into effect on 25th May 2018 and although the legislation is now in place, there are still many uncertainties and misconceptions.

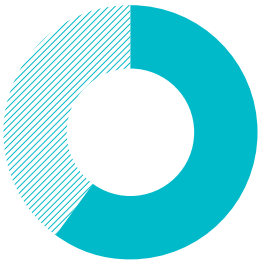
This is especially true in the payments industry where it is possible for complex layers of gateways, PSPs, acquirers and alternative payment suppliers to be involved in a single transaction.

Add to this the fact that globalisation gives even small merchants the option to sell internationally, it becomes clear, as acknowledged under recital 6 of GDPR, that GDPR compliance can be very challenging. Recital 6 says, ***'Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.'***

The downside of this is that hacking is becoming more and more interesting for criminals. The amount of data that can now be retrieved through a hack may be both immense and of tremendous financial value. Trends show a huge increase in data breaches and research shows that most companies do not have their house in order having poor cybersecurity practices in place.[1] Not only are the number of hacks going up, incidents are of increasing severity too (as concluded by several reports).[2] 60% of a pool of 1,250 executives and security practitioners are of the belief that an attack will hit their company in the next few years.[3]

In his welcome remarks at a conference in November 2018, Benoît Coeuré, member of the Executive Board of the European Central Bank said,[4] :

> "The next financial crisis may well start as a cyber-incident. In recent years these have grown rapidly in scale, scope and sophistication. Failure to adequately protect against cyber-attacks may have far-reaching repercussions. Digitalisation is the breeding ground for cyber-threats. Despite its undisputable benefits, digitalisation brought many ills, such as hacking, phishing or identity theft and in general it is an enabler of new forms of fraud. And the stakes have risen. Hackers increasingly target wholesale payment systems and the large money flows they handle. "



60%

of a pool of 1,250 executives and security practitioners are of the belief that an attack will hit their company in the next few years.

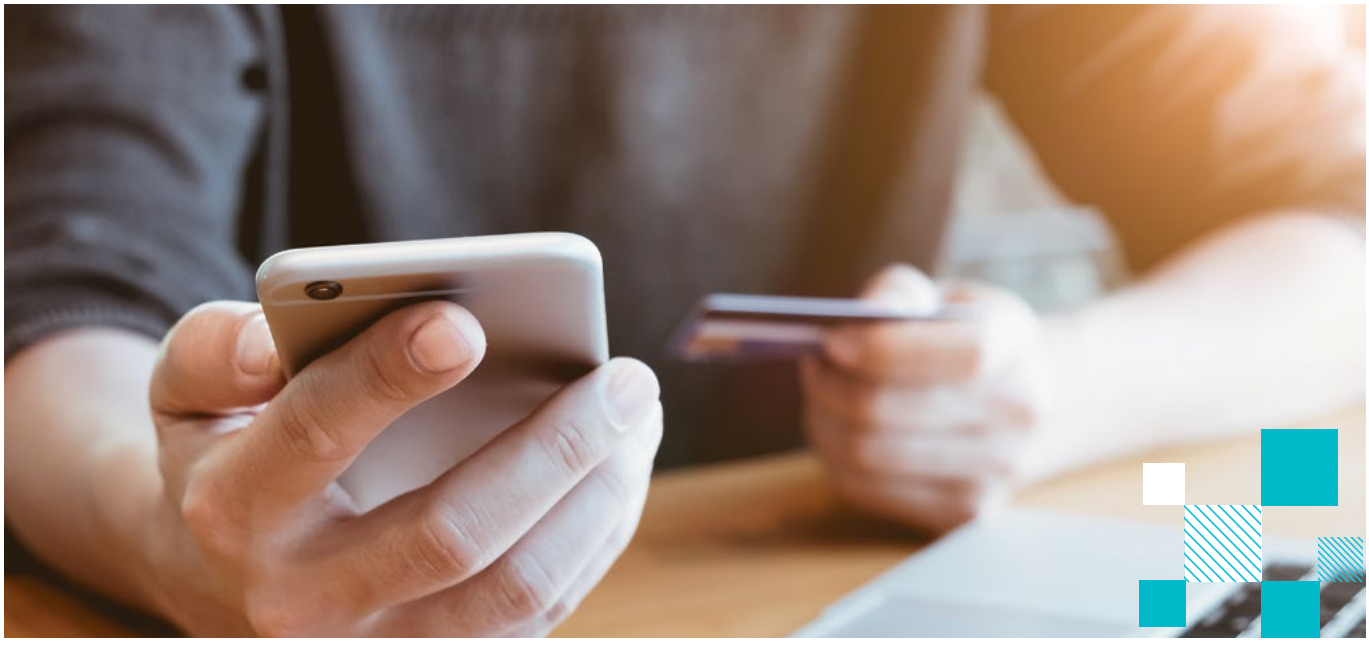
AIMS OF THIS WHITEPAPER

This whitepaper aims to give non-EU based merchants an understanding of the most common GDPR related questions and enable them to analyse their own compliance position and that of other related parties.

It also provides specific answers to questions that make the payments space complex including questions about GDPR compliance, server locations, hosting, documentation and the involvement and compliance of the many different parties within the chain of a payment transaction being made.

As validated by Ingenico ePayments with its key customers, the following top 10 are the questions bothering the minds of merchants based outside of Europe. These are addressed in this whitepaper:

1. What are the GDPR principles in summary?
2. As a merchant, if my PSP hosts the payment page, am I a controller or processor and what is the requirement?
3. Is my payment service provider a controller or processor?
4. Are payment players (acquirers, APMs and card schemes) processors or controllers?
5. What does the role of each player in the chain mean for me as merchant?
6. Would I be liable following any GDPR failures by my PSP or other payment players in the chain?
7. What actions are merchants advised to take to ensure they are compliant with GDPR when the PSP is hosting their payment page?
8. If a merchant works with several different PSPs, would this result in a different approach to GDPR compliance for each?
9. Does GDPR apply to me even if I am based outside the EU?
10. What key paperwork is required to ensure compliance with GDPR?



EXECUTIVE SUMMARY

GDPR sets ground rules for processing of personal data which includes almost every access to such data. Companies that process personal data subject to GDPR, should consider how they use the data. This is because rules apply about lawful and fair processing, being transparent to the data subjects, data minimisation, storage limitation, integrity and confidentiality. Finally, data controllers are held accountable and responsible for being able to demonstrate compliance with GDPR.

GDPR could potentially apply to merchants based outside the European Union if they actively target European customers. The determination of when active solicitation takes place is based on several factors. The European Data Protection Board (EDPB) has recently issued draft guidelines on extraterritorial applicability of GDPR, which is now pending consultation from stakeholders. The Guidelines provide a non-exhaustive list of factors that may indicate an intention to offer goods or services to individuals in the EU: running marketing campaigns aimed at an EU audience, using EU-related URLs, local contact telephone numbers for individuals in the EU, the website in a local language or offering payments to be made in a local EU currency. The mere accessibility of a website from the EU is insufficient. For the payment landscape specifically, I would say that the offering of a local payment method would also be relevant. It does not mean however, as clarified by the EDPB, that one of the factors taken alone is a clear indication that the merchant is indeed selling into the EU, however ***"they should each be taken into account in any in concreto analysis in order to determine whether the combination of factors relating to the controller's commercial activities can together be considered as an offer of goods or services directed at data subjects in the Union."*** Fully understanding this remark, you may wondering though whether this will lead to many different local interpretations (there is no clear threshold that for instance 3 factors of the EDPB criteria would suffice in order to conclude there is an offer of goods to EU data subjects, it might even be that a local authority believes 4 of the factors should be fulfilled before EU offering can be concluded to take place) and potentially non-EU companies being advised to make slight adjustments to their website to ensure their websites fulfil less of these factors, even though they internally know that they are offering goods/services to EU data subjects. We will need to wait and see how this will play out.

In the payment landscape, multiple parties are involved and it is not always clear which role each party takes. Are they data controller or data processor? The industry also seems unaligned. European guidelines however, do seem to lean towards the classification of almost all financial institutions (PSPs, acquirers, payment method suppliers and card schemes) as data controllers rather than processors. This may have severe implications to merchants, because they are at the forefront and they're the ones that hold the relationship with the data subject in question.

A new concept is seemingly emerging within the industry which is the idea of 'co-controller'. A party's claim to this is that two parties can both be controllers. They will consider therefore their own purpose; and they will not be joint controllers and they will not liable for each other actions. It is yet to be seen however, if this will stand up in court.

Unfortunately, a merchant not capturing personal data in the first place (for instance when making use of a PSP's hosted payment page) is not eliminated from this risk. They may still be deemed to be the data controller.

If a data breach occurs, it is expected that the data subject will turn to the merchant. As a controller, they are liable regardless who caused the data breach. However, GDPR provides an escape clause, as it says the merchant will need to prove that it is not in any way responsible for the event that gave rise to the damage.

The documentation required for GDPR compliance requires some time and effort to get right, but plays an important role in ensuring each organisation and individual meets the Regulation.

Documentation starts with the mapping out all data flows and recording processing activities. This also requires a good review of systems and tools that companies use and what those companies do with the data (where they store it, etc.). Think of Dropbox, your CRM system, your customer service ticketing system and internal communication tools like email and Slack. More tools store personal data than you may initially think of.

Further, paperwork may include (depending upon circumstances) a data protection policy, a privacy policy and a data protection impact assessment. Finally, depending upon to whom, their role and to which country transfers occur, a data processing agreement between parties may be required.

CONCLUSION OF THIS WHITEPAPER

Year by year personal data collection is increasing, making data more and more valuable. With this also comes a downside as criminals are becoming increasingly interested in and adept at hacking systems and stealing data. As a result, data breaches are almost becoming daily news.

Minimising collection, access, use of, or other form of data processing (including safe encryption of data, archiving historical data to offline environments and deleting data that's no longer needed) will not decrease the impact of GDPR on an organisation. These actions will however decrease the reach of any data incident and substantially limit the financial consequences and impact of any data breach if (more when than if!) it happens.

Companies should see GDPR as a sign of what the future holds and take data protection (and a robust approach to data management) seriously. It is not merely an IT issue to be ticked.

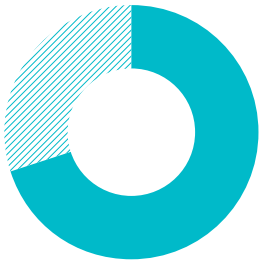
Data protection principles must be embedded throughout the entire organisation and, as GDPR states, 'privacy by design' is a must. Regardless of a company's geographic location and its role in any payment chain, all organisations should embed GDPR principles within their day-to-day working. From a reputational perspective, having to publically deal with a data breach is everyone's worst nightmare; it is uncertain what impact it will or will not have to a company's reputation. The results could be a significant financial impact including penalties, loss of customers and loss of shareholder value. Indeed, research shows that 70% of consumers would stop trading with a business following a data breach.[5] Even though surveys show that a majority feel that a data breach is inevitable. Due consideration should be given to the company's power to make life hard on hackers and to limit the amount of data they can take or use.

It is therefore time for each organisation to make cybersecurity part of its strategy and budget and not to try to save costs on it. A regular saying from wise compliance professionals is, "If you think compliance is expensive, try non-compliance."

GDPR and any future similar data protection legislation in other jurisdictions that may be introduced, requires an ongoing commitment.

European based PSPs and acquirers that operate with merchants based outside Europe can play an active role in ensuring the concerns of those merchants around GDPR are addressed. They have the skill set and the resources that small business merchants won't have (increasingly the ones that are under attack[6]). This could include alerting the merchants to GDPR applicability when they see local website URLs, website content in a local language and the selection of local payment methods.

This could also constitute providing advice on data minimisation, the requirements of a privacy policy and being transparent and open about its own GDPR compliance (that could assist merchants meeting their own compliance requirement). PSPs and acquirers should work together with the merchant's IT and security professionals to protect data as a primary business value.



70%
of consumers would stop trading with a business following a data breach.

INTERPRETATION OF THE GUIDANCE

The GDPR guidance that is currently available is limited and as a result, companies often interpret their requirements too literally. This leads to unease about compliance. ***Compliance (and gaining a clear understanding of how GDPR operates in the payments landscape) is even more challenging for merchants based outside the EU.***

On national and global levels, the collection and sharing of personal data (a definition that is extending in scope due to the ever-increasing expansion of data on natural persons being collected by companies[7]) has increased significantly.

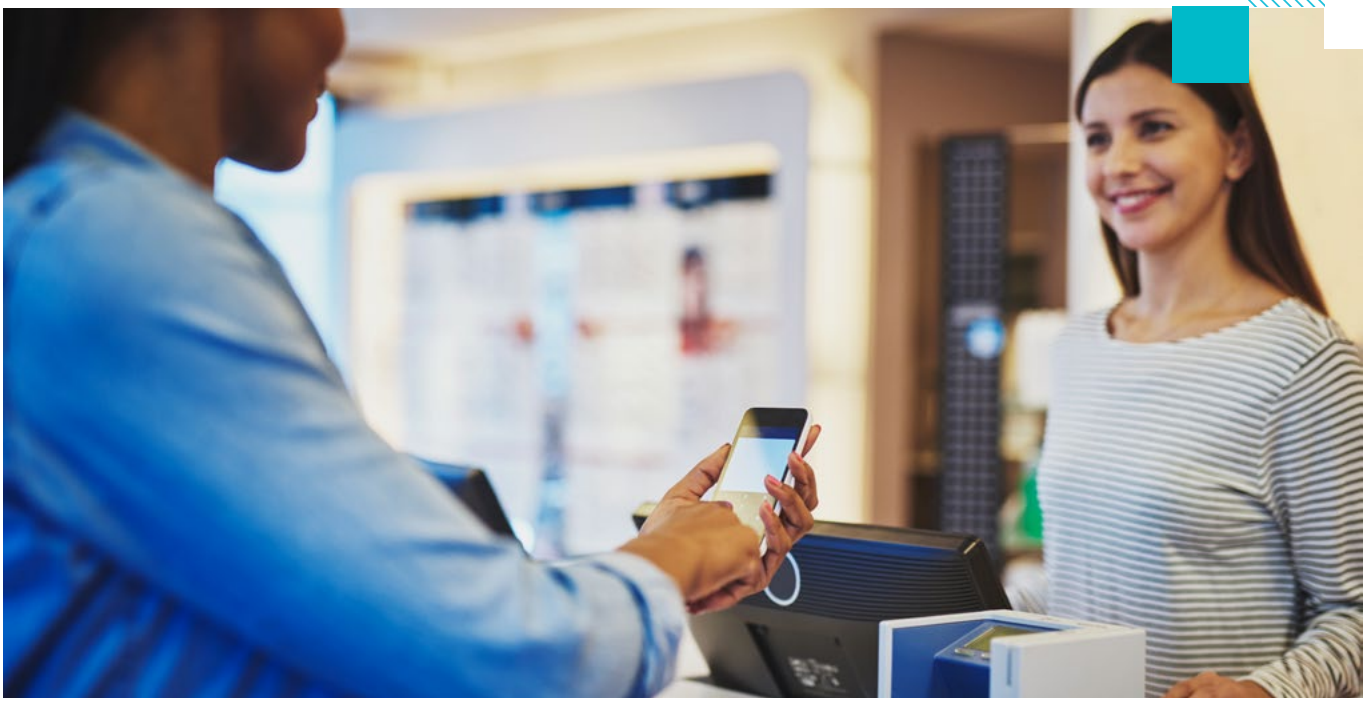
Recitals of the GDPR acknowledge that responsive technology is allowing companies to make use of data on an 'unprecedented scale in order to pursue their activities'.[8]

On the back of GDPR, data is therefore becoming currency. Indeed, some now say personal data is potentially more valuable than oil.

In our consumer-driven world, online customers expect increasingly to be pampered with personalised discounts, comparisons and offers based on their historic purchases.

Collection of data by quantity is also increasing and as a result, non-personal data may become personal if (as technology enables) it is combined with other data.

Not surprisingly, these developments result in many new challenges when it comes to the gathering, protection and use of personal data.



ROLES THROUGHOUT THE PAYMENT CHAIN

We begin by looking at the position of players and at some key terminology and in particular the roles of data processor and data controller.

A party that processes personal data is either a data controller or a data processor. A data controller is a party that (alone or jointly) determines the purposes and means of the processing of personal data. A data processor is a party that processes personal data on behalf of the controller, for the purpose as determined by the controller.[9] However, the determination and distinction between roles, especially in the world of payments, is not straightforward.

In reality, the role an organisation holds in the payment chain determines to what extent it must comply with GDPR and to what extent it can be held liable (by law) for any failure. It is very important to make an appropriate assessment of each party to determine if it should be classified as data controller or data processor.

Using the existing available guidance from the UK Information Commissioner's Office, the European Data Protection Board (previously known as The Article 29 Working Party) and the Card Schemes, this whitepaper explains the difference between the two parties.

It is advisable however, for merchants and processors to seek their own legal advice and this is because a variety of circumstances play a determinative role.

Since the role definitions have not been altered compared to GDPR's preceding directive (and unless the Data Protection Board explicitly revokes its guidance) this white paper also takes guidance from the so-called SWIFT opinion issued in 2006.[10]

Controller & Merchant

The controller is the organisation that decides which data to collect, how it is used and with whom it is shared. This sounds easy to determine however, in the world of payments, it may not be.

First and foremost, a merchant must determine its own role and position in the payment chain.

Merchants receive personal data that originates from a person making a purchase at the merchant's website for its goods or services (some of the data that is required will need to be included in the transaction data that is forwarded to the merchant's payment service provider).

Therefore, the merchant determines the purpose of processing and also with whom the data is shared. It is therefore considering controller.

QUESTION 1

WHAT ARE THE GDPR PRINCIPLES IN SUMMARY?

GDPR is driven by the simple adage that, ***'The processing of personal data should be designed to serve mankind.'***[11] The legislator apparently had a philosophical moment while drafting GDPR.

Most importantly, GDPR enhanced the earlier rights of data subjects in a number of ways. For example, data subjects now have the right of data portability (the right to transmit data to another controller without hindrance from the controller, to which the personal data has been provided) and the right 'to be forgotten' (the right to require deletion of personal data kept).

Organisations subject to GDPR are therefore required to make sure they are able to accommodate the rights of data subjects if they are processing or retaining their personal data. They must fully understand their processing of personal data and the ways in which they make it available and make easy for the individual to change service providers (data portability).

We have seen a number of high-profile data breaches and unauthorised disclosures in the past. If you are a data controller, you may need to report a personal data breach under the circumstances set forth under GDPR (known as a data breach notification) to the appropriate supervisory authority without undue delay. Where feasible, this must be no later than 72 hours after having become aware of it. This gives you the responsibility to monitor your own environment for breaches and to notify regulators and affected individuals (when required) as required under GDPR.

Organisations may also need to appoint a Data Protection Officer (DPO). It is the role of a DPO to supervise and advise upon the security management of personal data kept and to manage other issues relating to the processing of personal data.

Organisations may also need to conduct a Data Protection Impact Assessment (DPIA).These assessments need to be made available to the supervisory authority upon request. These must identify data handling procedures and processes as well as the controls in place to protect and manage personal data.

Recital 114 of GDPR tells us, ***'The controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.'***

One solution for this is parties to enter into a Data Processing Agreement (DPA) or the standard contractual clauses as approved by the European Commission. These can be signed between a controller and processor as an authorised transfer mechanism, particularly if personal data is transferred outside the EU by the organisations. Other transfer mechanisms that could be utilised, are the standard contractual clauses issued by the European Commission, binding corporate rules or an approved code of conduct.

These documents exist to ensure that each data processor meets the requirements of GDPR. A DPA (or the standard contractual clauses) will not be required however, if the European Commission determines that a country has equivalent safeguards and an adequate level of data protection.[12] Currently, adequacy decisions have been given to (amongst others) the USA (the Privacy Shield Framework), Canada and New Zealand. Japan has recently been added and safeguards are pending within South Korea.[13]

Under their responsibility, both controllers and processors are required to maintain a record of (all categories of) processing activities.[14] These records should contain (for controllers):

- Name and contact details for the controller
- The purposes of processing
- Description of categories of data subjects
- The categories of personal data processed
- The categories of recipients (and whether or not they are based in third countries outside EEA)
- The suitable safeguards taken (such as the DPA)
- The time limits for erasure
- A general description of the technical and organisational security measures (where possible).

For data processors, the list of requirements is shorter, but not to be neglected either.

Lawful, fair and transparent

Any processing of personal data should be lawful and fair.

It should be transparent to natural persons how personal data concerning them is collected, used, consulted or otherwise processed and also to what extent this personal data is (or will be) processed.

The principle of transparency requires that any communication relating to the processing of personal data should use clear and plain language and therefore be easy to access and understand.

The principles of 'lawful, fair and transparent' concern in particular, information about data subjects on the identity of the controller and the purposes of the processing and also information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and the communication of personal data concerning them.

Natural persons should also be made aware of risks, rules, safeguards and their rights in relation to any processing of personal data and how they can exercise their rights. In particular, the specific purposes for which personal data is processed should be explicit and legitimate and also determined prior to the time of collection.

Further, the personal data should only be adequate, relevant and limited to what is necessary for the defined processing purposes and only processed if the purpose of the processing could not reasonably be fulfilled by other means.

In particular, this requires ensuring that the period for which personal data is stored is minimised and limited. In order to ensure that personal data is not retained longer than necessary, these time limits are determined by other laws or otherwise should be established by the controller (giving a time and date for erasure or periodic review).

In addition, every reasonable step should be taken to ensure that any inaccurate personal data is rectified. A data subject also has the aforementioned 'right to be forgotten' and to require rectification.

AS A MERCHANT, IF MY PSP HOSTS THE PAYMENT PAGE, AM I A CONTROLLER OR PROCESSOR AND WHAT IS THE REQUIREMENT?

If the above hosting premise applies to you, this effectively means that the merchant does not collect any transaction data. Therefore, there is no transfer of data from the merchant to its PSP. The PSP therefore, handles direct collection of such data without interference from the merchant.

Also, it will be the case that the PSP will determine the different data fields on the payment page. However, could this mean that the merchant is then no longer processing personal data subject to GDPR and/ or no longer a data controller?

No, this is not the case, ***as the merchant is still making important decisions relating to the processing and remains therefore, a data controller.***

As the establisher of the (purchase) relationship with the customer, it is still the merchant that decides how the data is used and with whom it is shared. The merchant is the organisation that decides to collect in the first place and determines the legal basis for doing so. The EDPB clarified (in its 2010 Opinion) the roles of processor and controller. It determined that, ***'Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.'*** It also determined the purpose, which individuals to collect about, whether to disclose the data and to whom. The fact that initial collection (through a hosted payment page) is not done by the merchant but its PSP, does not change the designation.

Further, in the above question, processing is still occurring on the merchant's side even if the PSP hosts the payment page. ***The definition of 'processing' under the Regulation is extremely broad. Not only does processing constitute the collecting or transmission of data, it also involves the retrieving, use of, or otherwise making data available.***[15]

The merchant would still access and use personal data through the PSP's systems and reporting (in order for example, to reconcile payments, initiate refunds and challenge charge-backs). In addition, even if there is no processing of personal data by the merchant, it would necessarily have to alter its position as controller. This is made clear in a recent judgment of the European Court about the operator of a Facebook page.[16] Even though the page operator only received anonymised data from Facebook, it played a role in the determination of the purpose and the means of processing (jointly with Facebook, therefore the criteria for data collection and anonymisation were determined). The fact that the responsibilities of both parties were unequal was deemed irrelevant. Facebook and the page operator were considered joint-controllers. This concept will be revisited later within this white paper.

IS MY PAYMENT SERVICE PROVIDER A CONTROLLER OR PROCESSOR?

The PSP processes payments and redirects transaction data to the relevant acquirer/ payment method supplier. Are they therefore just following the merchant's instructions while processing the payments?

Some players in the market say they do and therefore, they are simply a processor. Some PSPs however say they do more than just that (an example of this may be Ingenico ePayments).

The key issue in terms of defining the PSP's role is the extent to which a controller has responsibility for (and freedom to determine) the overall processing activities.

Let's take some guidance here from the SWIFT opinion. SWIFT considered itself to be a processor in 2006 when the Data Protection Board (back then, the Article 29 Working Party) was assessing their position. When in 2006, the Article 29 Working Party analysed the data processing activities of SWIFT, it determined that SWIFT, together with its financial institution clients, was a controller (sharing joint responsibility as data controller although in different degrees) in relation to the personal data it processes. Applying the SWIFT analysis could just as readily lead to other service providers being characterised as data controllers in circumstances that they had not anticipated.

The SWIFT example highlights a number of responsibilities that the organisation had taken on with regard to its processing operations. These were considered by the Board to be going, ***'beyond the set of instructions and duties incumbent on a processor and cannot be considered compatible with its claim to be just a processor.'***

The instructions and duties include the ability to:

- Decide autonomously on the level of information that will be provided to financial institutions in relation to the processing
- Determine the purposes and means by developing, marketing and changing the existing (or new) SWIFT services and the processing of data. For example, by determining standards applicable to a client as to the form and content of payment orders but without consent from the financial institutions
- Provide added value for processing such as the storage and validation of personal data and the protection of personal data with a high security standard
- Take critical decisions with respect to the processing; such as the security standard and the location of operation centres
- Negotiate and terminate with full autonomy, service agreements
- Draft and change various contractual documents and policies.

Significantly, as they often have the ability to choose the composition of the portfolio of services they use (services are developed and changed and value-added services are supplied to enable them to stay ahead of competition and to bind existing customers) these factors apply to many payment companies.

Payment companies also have the ability to, beyond the sole acceptance of instructions from the controller, develop the software they use to supply services and make critical decisions.

This can include the ability to impose additional requirements on merchants by means of its software, but without the merchant's consent.

Is it not however, the case that most payment processing company have these powers. If for instance, a controller gives a processor detailed instruction, there is little margin of manoeuvre for the processor.

A party that monitors another party's performance and compliance within the contract (and any required technical and organisational measures) may also be help in the determination of the status of the first party.

This indicates that the controller is in full control of the processing activities.

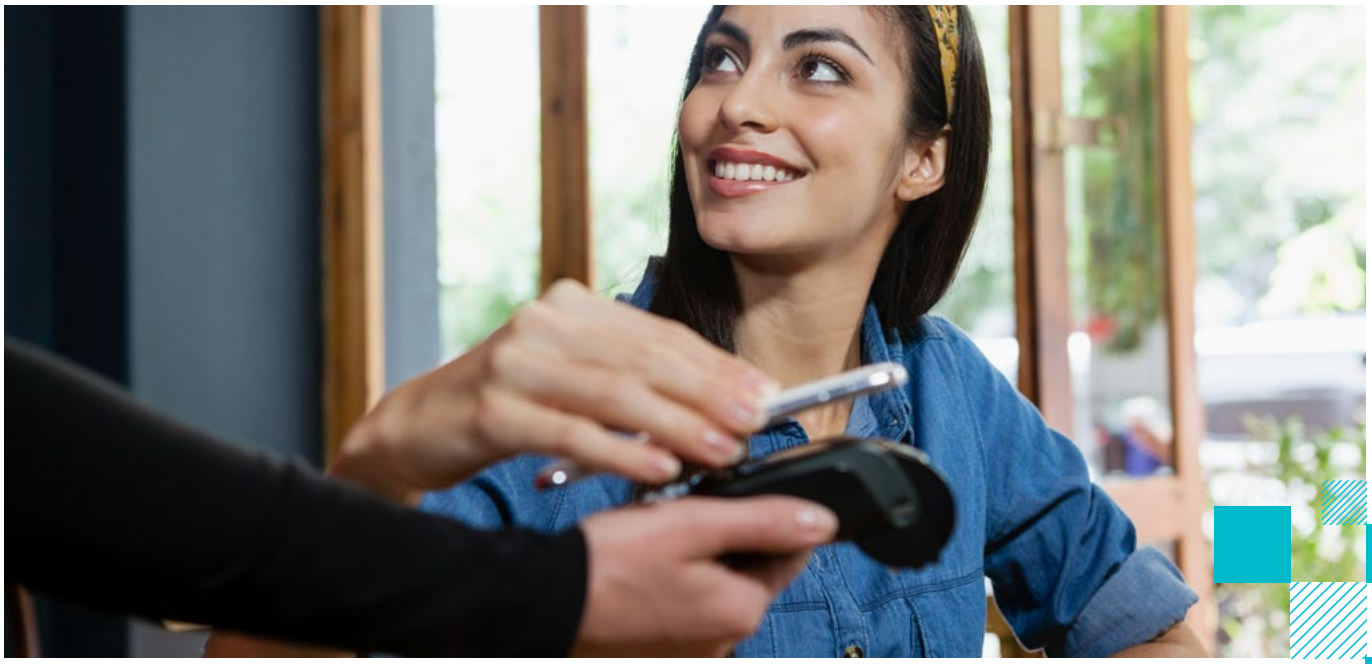
However, these points alone cannot be solely relied upon. There are often situations in the payments industry where a processor exceeds the mandate given by a controller and actually plays a role in determining the purposes for which the data is processed.

The payment chain continues to fragmentise, making added value services key for market players. However, these add-on services, as shown above, may also prove that a party's assumption that they're a processor, to be wrong.

Even though the particular service offering and the circumstances of each PSP play an important role in deciding whether or not they are processor or controller, it seems that the typical PSP would be deemed a controller. Taking into consideration the role of PSPs as intermediary in the chain between merchant and acquirers (with its value-added services) it is not feasible to claim that the merchant has exclusive control over the purpose for which the data is processed, the content of the data or what the data will be used for.

A key consideration (as stated by the UK ICO) is asking, who exercises controller over the content of the personal data? It is the PSP that decides which information it needs to process payments correctly, even if it is jointly working with the other players in the chain. See below for more details.

Now we look at the position of acquirers/ alternative payment method suppliers.



QUESTION

ARE PAYMENT PLAYERS (ACQUIRERS, APMS AND CARD SCHEMES) PROCESSORS OR CONTROLLERS?

The guidance as deemed relevant for a PSP's determination, may apply to others in the chain as well.

Further, the 2010 Opinion provides various examples on companies processing data and the determination of their roles.[17] This includes where financial transactions are processed (Example 10).

The given example stipulates a situation where a bank uses a financial messages carrier in order to carry out financial transactions. Both the bank and the carrier agree about the means of processing (they agree the processing is carried out at a first stage by the financial institution and only at a later stage by the carrier).

The EDPB determined that, ***'Even if at micro level each of these subjects pursues its own purpose, at macro level the different phases and purposes and means of the processing are closely linked.'***

The final EDPB verdict was, ***'In this case, both the bank and the message carrier can be considered as joint controllers.'***

Applying this example on an analogue basis to the entire payment industry (where PSPs and acquirers are the bank and the card schemes are the financial messages carrier) we may even wonder whether there would be any party in the chain that could rightfully claim to only being a processor. On the basis of this guidance you may conclude that all payment players in the chain are controller, and all serving the same purpose and determining the means of processing together, they could even more so be considered joint controllers. This would imply responsibility for one another as the data subject may exercise his/her rights under GDPR in respect of and against each of the controllers. See further on this the next question.

However, relevant criteria highlighted by the EDPB also includes the expectations of the data subjects. The criteria is, as set by EDPB, ***'If the controller is highly visible to data subjects then it is less likely that the processor will have a co-controller role.'*** This makes it even more complex where in a payment chain it is highly possible that a buyer has no knowledge of the processing parties involved (that do not issue the credit card or alternative payment method) and have no contractual relationship with the individuals such as the PSPs. It is unclear which criteria has overruled which. It is also not certain whether the co-controller relationship (each party is controller but has their own purpose for processing) will stand ground in the payments industry. Perhaps, the industry requires a very specific test case (and one involving all players) to be ruled out in court, to give us all clarity.

What's more, in the case of issuers and alternative payment method providers, they have their own relationship with the customer. Therefore, a definition as a mere processor would not seem suitable for them.

Irrespective of a party's conclusion on its role, GDPR introduces an accountability principle which requires each organisation to show that it has made this evaluation, and also what arguments it considered before it came to its final conclusion. It should be noted that no explicit administrative penalties have been provisioned within GDPR for wrongful determination by a party of its role. On the other hand, controllers do have some further responsibilities and failure to adhere because a party believed it was a processor could have impact. ***Further, as some of the basic transparency principles are involved (a data subject for example, must be aware of all controllers of their data and therefore mentioned in the privacy policy) players must be extra cautious because breaches of adherence to these principles carry potential fines of up to four percent of the total worldwide annual turnover.***

Let's now look at the impact for merchants.

QUESTION

WHAT DOES THE ROLE OF EACH PLAYER IN THE CHAIN MEAN FOR ME AS MERCHANT AND WOULD I BE LIABLE FOLLOWING ANY GDPR FAILURES BY MY PSP OR OTHER PAYMENT PLAYERS IN THE CHAIN?

Based on the above, it is possible to conclude that under GDPR, the merchant as well as its PSP, the credit card acquirer, the issuer and the card scheme provider could all be considered to be controllers.

They may all therefore be considered to be liable towards the data subject if a data breach occurred, regardless whose fault it is. For merchants this can be a major concern.

Article 26 of GDPR explains the concept of joint controllers and says, ***'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. Irrespective of the terms of the arrangement…. the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.'*** Being joint controllers brings legal consequences.

As clarified by the European Commission; ***'Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed.'***[18] Joint controllers are acting together to decide the purpose and manner of processors. Not every controller-controller relationship is a joint one, it is possible that they simply share a set of personal data that they process independently of each other, often referred to as co-controllers rather than joint controllers. The idea is that two parties can both be controllers, but that they consider therefore their own purpose for processing. Therefore, they will not be joint controllers and they will not liable for each other actions. The distinction is very hard to make in the real world however and you may wonder if it is possible in the space of payments to say each payment company, while processing one payment transaction, determines their own purpose. Is there not only one purpose when parties are processing data as part of a payment transaction: to clear and settle the transaction? There might be other underlying purposes like to perform screening to ensure AML compliance, but the main purpose is to get the merchant paid for a service or good delivered.

The PSP, acquirer and card scheme together jointly determine the purposes and means of processing in that respect. It seems hard to argue that they each have their own purpose independent from each other and therefore the co-controller concept seems not to work in the payment industry. At least, the different phases and purposes are closely linked at macro level, rendering the argument of co-controllership flawed. If parties are all considered controller, the obvious implication would be that they are all considered joint-controllers.

Further, in terms of liabilities, Article 82 stipulates, ***'Where more than one controller or processor or both a controller and a processor are involved in the same processing and where they are under paragraphs 2 and 3 responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.'***

Could this mean that the merchant will have to compensate its customer for full damages if another party in the payment chain caused the damages?

The article also refers to other paragraphs in Article 82 under which a controller (or processor) is responsible first. Paragraph two lays down liability for a controller in case it infringes this Regulation.

The escape is however given where it states, ***'A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.'***

Thus, it may be that the merchant will not be held liable for data breaches from its PSP or acquirer, but it will need to be able to prove in court that it is not responsible.

If trade is across borders, the data subject (the merchant's customer) may file court proceedings against the merchant in the data subject's home country.[19]

Legal proceedings such as this would result in the merchant having to incur legal and court costs and also potentially internal resource costs to enable them to address the matter and build a defence.

And even after court proceeding are concluded, if the merchant is proved innocent, who will compensate for all the costs they have incurred?

Ideally for the benefit of the merchant and the sake of the relationships, the responsible party (the PSP or acquirer for instance) if they caused the damages incurred by the merchant's customer, should be required to act and address their error and relieve the merchant from unwanted burdens.

A controller or processor that has been ordered by the court to pay full compensation for the damage suffered, shall be entitled under GDPR (even if there is no contractual right given) to claim back from the other controllers or processors involved, the compensation corresponding to their responsibility for the damage.

This could potentially also include costs incurred by the merchant in defending its case.

It is clear that understanding which jurisdiction would be eligible could be a significant issue. In seeking clarity, GDPR states that blame should lie either where the controller or processor has an establishment (as a non-EU merchant would the location of its EU representative count?) or where the data subject has residence.

However, in a controller-controller or controller-processor case, when claiming for damages paid, there will be no data subject involved.

The industry is therefore waiting to hear the first court ruling in relation to a case like this.

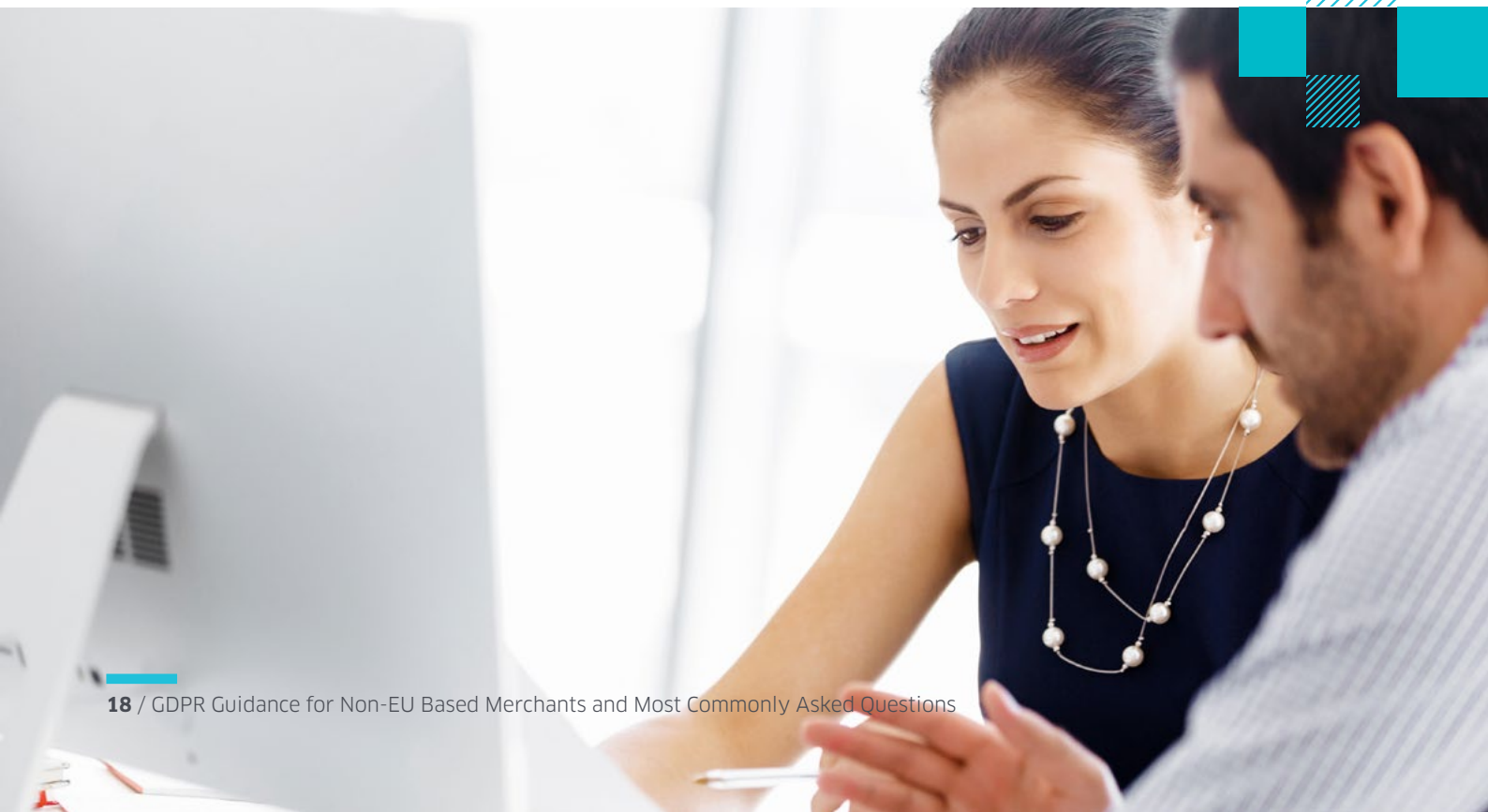
QUESTION 6

WHAT ACTIONS ARE MERCHANTS ADVISED TO TAKE TO ENSURE THEY ARE COMPLIANT WITH GDPR WHEN THE PSP IS HOSTING THEIR PAYMENT PAGE?

As explained above, a PSP, when holding the payment page does not change the merchant's role from itself being a controller to being a processor.

Here the merchant is still determining the purpose of processing and will, through the PSP's system, obtain access to the transaction data even if this is not made available at the start of the transaction within a payment page.

In terms of the actions merchants are advised to take, ***all the above responsibilities as laid down for controllers will apply to merchants, regardless of who hosts the website payment page.***



QUESTION 7

IF A MERCHANT WORKS WITH SEVERAL DIFFERENT PSPS WOULD THIS RESULT IN A DIFFERENT APPROACH TO GDPR COMPLIANCE?

A merchant working with a number of PSPs purely adds more parties to the list of whom they transfer data to (they must ensure that these are detailed in their records of processing activities!).

In principle this does not therefore, result in a different approach to compliance but it does make compliance more burdensome and complex.

As detailed above, GDPR remains highly challenging, especially within the complex payment chain.

As stated, some PSPs/ acquirers deem themselves controller and others believe themselves to be processor and this confusion has impacted on the entire interaction between a merchant and its processing partners.

Each relationship (controller/ processor vs. controller/ controller) has to result in a different approach; in particular with regard to the agreement and contractual language being put in place.

Discussions around this, most commonly to agree on the responsibilities and status of each party, can be lengthy and frustrating. As a result, disagreements are not uncommon.

However, as soon as clarity is achieved, business can continue.

DOES GDPR APPLY TO ME EVEN IF I AM BASED OUTSIDE THE EU?

For non-EU residents, Recital 14 of the Regulation states, ***'The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.'***

GDPR applicability is therefore based on certain determining geographical factors and in order to ensure that natural persons are not deprived of the protections to which they are entitled (as emphasised within the Regulation), it applies to all organisations based within the EU regardless whether or not the processing itself takes place within or outside the EU.

In addition, any organisation with no establishments in the EU but processing personal data of EU data subjects is also required to comply.

To ascertain whether an EU-based company is indeed offering goods or services to data subjects in the EU, the legislation tells us that, ***'It is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union'.*** [20]

If they seem bound to undertake active solicitation of EU customer, then this is a factor that is often considered in determining applicability of local laws (in Europe).

Thus, if a merchant has a .com website in the English language (provided it is a common language generally used in the merchant's country of establishment) which can be accessed by a customer in the EU, this does not necessarily result in GDPR applicability.

Circumstances such as this are considered to be insufficient to ascertain the intention to actively solicit EU customers.

If a non-European merchant offers a website (for instance in a language which is not generally spoken in that merchant's country) or offers the possibility to pay with EUR, this may make it apparent that the merchant does undertake to offer goods or services to consumers in the EU.

GDPR therefore applies.

Generally, any mention of customers or users in the EU is likely to lead to the conclusion of GDPR applicability.

QUESTION 9

WOULD GDPR APPLY TO ME IF I MAKE USE OF AN EU-BASED PSP EVEN THOUGH I SELL MY GOODS/ SERVICES ONLY TO NON-EU CUSTOMERS?

Prior to GDPR there was a risk of non-European merchants being subject to the European Data Protection Directive if they were making use of a European-based service provider (the rule of having equipment based in the European Union would trigger applicability of the European data protection rules).

Now with GDPR in place, if a merchant uses an EU-based PSP or acquirer for processing of transactions, even for non-EU based customers, then this no longer constitutes a risk for them under GDPR.

The territorial ruling within Article 3 clarifies that ***GDPR applies if a controller or processor has an establishment in the EU, regardless of whether it concerns processing of personal data of EU citizens or not.***

When it comes to non-EU based companies, the rule of offering goods and services to EU citizens (as discussed above) also applies.

The rule also applies if behavioral monitoring of a subject takes place within the EU.

Therefore, non-EU based merchants offering goods or services to non-EU customers do not fall within scope of GDPR, even in cases where its PSP or acquirer(s) are based in the EU. The European Data Protection Board has clarified in its draft Guidelines on Extraterritorial Application of the GDPR[21] that ***a non-EU controller that is not otherwise subject to the GDPR will not become subject to the GDPR merely because a data processor located in the EU processes personal data on its behalf.***

This does not mean that the PSP or acquirer does not need to comply with GDPR when interacting with its non-EU merchants and customers. The question would then be, 'What if the PSP or acquirer provides access to such non-EU merchant to the transaction data (including personal data)?' Would this not be considered a transfer to a third country for which one of the transfer mechanisms should be applied? If we look at the intentions of GDPR it can be concluded that this should not be necessary. Indeed, recital 101 stipulates that, ***'When personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations the level of protection of natural persons ensured in the Union by this Regulation should not be undermined.'***

However, conflicting with this is the next section which states, ***'In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.'***

The latter statement is also embedded in article 44 of GDPR, laying down the general principle for transfers. This article clearly says, ***'Any transfer shall take place only if the conditions are complied with.'*** Following the letter of the law (and a literal interpretation) this would mean a PSP would have its non-EU merchants (which are controllers) enter into data processing agreements if no other transfer mechanism can be applied.

As started previously, the complexity of the world of payments and the chain of data flows can result in some truly bizarre situations. In my view, a practical application of the law which also follows the spirit and intention of GDPR is needed. For this, I refer to the first part of the quoted recital that highlights, that the transfer should not undermine the level of protection of natural persons ensured in the Union.

The legislation was not intended to cover non-EU customer data processing by non-EU based merchants and therefore, no transfer mechanisms should be applied. However, it is yet to see if the EDPB agrees with this train of thought. There was an expectation that the aforementioned draft Guidelines on Extraterritorial Application of GDPR would provide guidance on restrictions on transfers of personal data outside the EU and the extraterritorial application of the GDPR, but the draft has not covered this. We may expect that the consultation will bring this issue forwarded to be resolved. We won't know more until these Guidelines are published in final form, which is expected by April 2019.

QUESTION 10

WHAT KEY PAPERWORK IS REQUIRED TO ENSURE COMPLIANCE WITH GDPR?

It is important to note that the paperwork is only half of what is required by organisations to ensure they meet GDPR compliance. This is never a straightforward 'tick the box' exercise and the amount of work involved should not be underestimated.

As a first, a company will need to start with a ***data protection policy.*** The data protection policy is for internal use and must describe how GDPR principles are to be fulfilled by the organisation. It must also define the grounds for data processing, how those involved will be trained, data retention periods, the technical and organisational measures that will be taken and also how cooperation with third parties will take place.

In addition, ***an external privacy statement on the website*** is required and this must include and detail all contact details of the merchant and any (joint) controllers, what personal data is processed and why, customer rights, details about any data being transferred outside the EEA and also which parties will be involved. Do not forget to include a cookie policy!

With regard to further documentation, a controller will in general need to have the following paperwork in place, but some of these may not always be relevant depending upon different factors: ***data processing agreements with processors*** (if no other suitable safeguards are present – see also Question 1), ***procedures to handle data subject rights and to handle a data breach.*** Further, if processing entails a high risk for the data subjects, ***a data protection impact assessment*** is required (see also Question 1).

CUSTOMER VIEWS COUNT

GDPR has not only increased obligations on companies processing personal data, but has also created an environment of more awareness and increased scrutiny by data subjects.

Customers have, quite naturally, started asking questions on what data is held on them and for what purpose.

Not surprisingly, the relationship between an organisation and their data subjects is being redefined.

This does not necessarily mean by the way, that consumers are no longer willing to share their personal data.

Research from GDMA, UK DMA and Acxiom on the impact following the introduction of GDPR found that 51% of respondents across four continents would share their personal data with business if there was a clear benefit to them in doing so.[22]

One in five people surveyed were categorised as data fundamentalists (people who are unwilling to share personal information under any circumstances).

Most importantly, over three quarters of those questioned (77%) said they have no fundamental objections to engaging in a so-called data economy.

However, even though there is a proven willingness to share data, it is worth noting that consumers often feel that they are not in control of the data they're asked to provide.

51%
of respondents across four continents would share their personal data with business if there was a clear benefit to them in doing so.

77%
over three quarters of those questioned said they have no fundamental objections to engaging in a so-called data economy.

GOOD PRACTICE

A merchant may choose to adjust its websites to prevent any suspicion of active solicitation of European consumers to stay out of the loop of GDPR.

However, there is no escaping it. More and more countries outside the EU are following GDPR's lead with local data protection laws being updated to include more rights and obligations for data subjects.

Together with its PSP(s), a merchant should take GDPR compliance into serious consideration and take appropriate action.

This shows their customers that they care about their data protection, regardless of residency.

Good merchant practice also includes having a re-assessment of the necessity of any data currently being requested from a customer when they are making a website purchase and active discussions between merchant and PSP on how to minimise impact if something does go wrong.

PSPs are the experts when it comes to security and technical measures (this also includes the acquirer). These sophisticated financial institutions are fully designed and equipped to handle sensitive data.

However, besides having the PSP host the payment page they may also need to agree to have reduced access to personal data.

All merchants should therefore, consider carefully the value as well as the use of a specific personal data field. Is the collection and retention of a subject's date of birth for example, truly necessary or could the year of birth or age suffice?

REFERENCE

1 https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf

2 https://www.varonis.com/blog/cybersecurity-statistics/

3 https://thecybersecurityplace.com/60-of-firms-believe-a-major-security-event-will-hit-in-the-next-few-years/

4 https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181115.en.html

5 https://www.cutimes.com/2017/11/29/70-of-consumers-would-stop-following-a-business-af/

6 https://blog.dashlane.com/data-breach-statistics-2018-forecast-everything-you-need-to-know/

7 Article 4.1 GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

8 Recital 6 GDPR

9 Articles 4.7 and 4.8 GDPR

10 https://iapp.org/media/pdf/resource_center/wp128_SWIFT_10-2006.pdf

11 Recital 4 GDPR

12 Article 45 GDPR

13 http://europa.eu/rapid/press-release_IP-18-4501_en.htm and https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

14 Article 30 GDPR

15 Article 4.2 GDPR: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

16 http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d8943c7595a9e54cb59d27c60354ea2d9f.e34KaxiLc3qMb40Rch0SaxyPaxz0?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1381444

17 https://iapp.org/media/pdf/resource_center/wp169_concepts-of-controller-and-processor_02-2010.pdf

18 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

19 Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.'

20 Recital 23 of GDPR

21 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

22 http://www.itpro.co.uk/data-processing/31901/has-gdpr-really-changed-the-relationship-between-businesses-and-their-data

AUTHOR

Nadja van der Veer

Nadja van der Veer is a payments lawyer with over 10 years of experience in the international Payments industry and a legal expert in rules and regulations involving PSD, AML and CDD and Card Schemes. As Co-Founder of PaymentCounsel (www.paymentcounsel.com) and one of the Managing Partners of Pytch Ventures (www.pytchventures.com) she consults Merchant Acquirers, Payment Services Providers (PSPs/MSPs), other Fintech companies and Merchants in their startup phases that want to expand their business internationally, while mitigating risk.

About Ingenico ePayments

Ingenico ePayments is the online and mobile commerce division of Ingenico Group. We unlock the power of payments to help businesses reach new markets, increase revenue and grow into the future.

For more information please visit:
ingenico.com/global-ecommerce

CONTACT US

EDITORS

John Chou

John Chou is global data protection officer at Ingenico ePayments and a certified privacy expert. He has a solid privacy advisory background at major firms where he primarily focused on GDPR implementation within the financial services industry. As data protection officer he informs and advises Ingenico ePayments on the data processing obligations as set out by relevant (international) laws, regulations, and internal policies; and monitors its compliance.

Nick Tubb

Nick Tubb is Vice President, Commercial Affairs for Ingenico ePayments, responsible for global sales and commercial strategy within our online and mobile payments division. As an experienced veteran of the payments industry, Tubb most recently spent two years as General Manager, Asia Pacific for the company, responsible for the region's business results, and prior to that established and ran the company's Professional Services group. Before Ingenico, he also enjoys a 13-year career in non-bank foreign exchange, leading business acquisition and growth teams in Europe, the US and Australia.