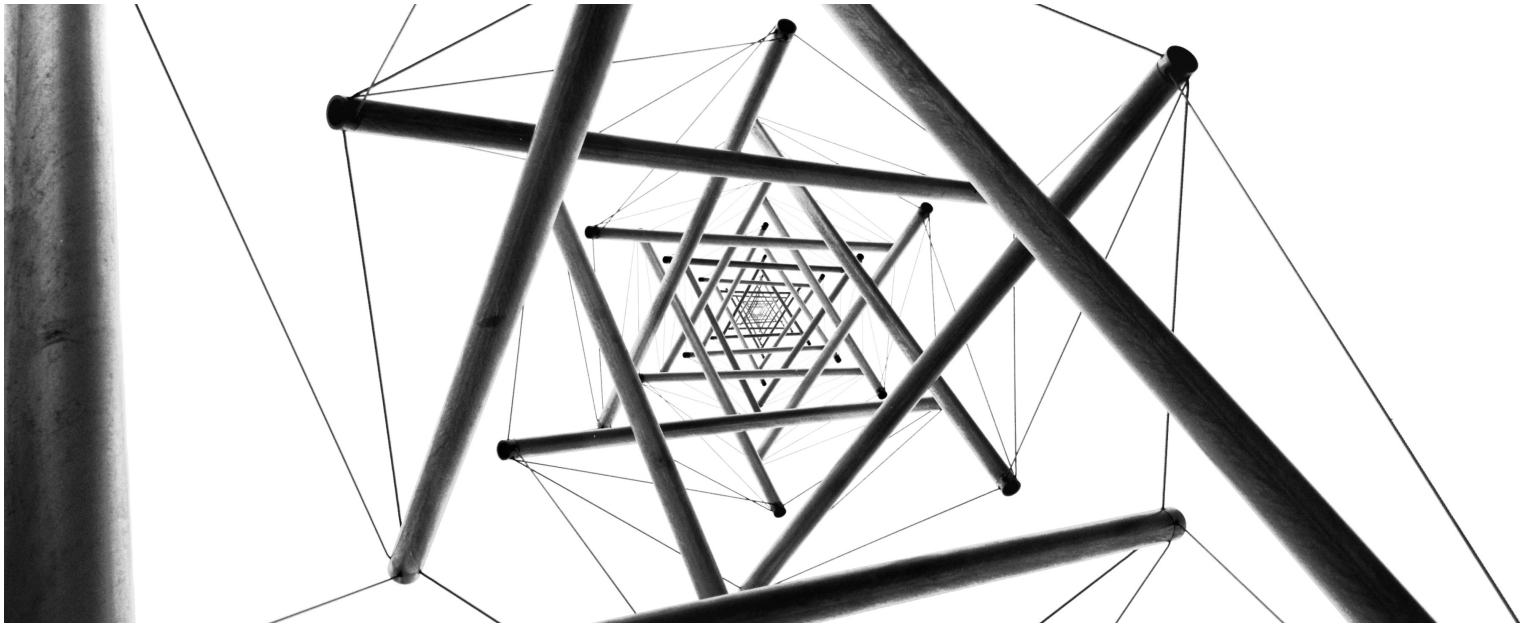
Feb 2019

EU: The interplay of PSD2 and GDPR - some select issues

It can be argued that the principle purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Payment Services Directive (Directive (EU) 2015/2366) ('PSD2') are in contrast with one another, as the PSD2 enacts data sharing requirements for financial service providers, whilst the GDPR gives individuals greater control over their data and restricts the freedoms to share it. Financial entities have therefore experienced concern with regard to overlapping provisions in the two pieces of legislation. Scott McInnes and Lupe Sampedro, of Bird & Bird LLP, provide insight into the key areas of overlap between the PSD2 and the GDPR, and share their views on how entities might navigate the same.



Dhruv Weaver/Unsplash.com

Issues have arisen at the interplay of the PSD2 and the GDPR. This is not surprising since, at the highest level, the objectives of the two pieces of legislation seem to contradict each other:

- The PSD2 is about requiring financial institutions that maintain payment accounts (so-called account servicing payment service providers ('ASPSPs')) to open up their infrastructure and give access to data (including personal data protected under the GDPR) to third party providers ('TPPs'). There are essentially two sorts of TPPs: account information service providers ('AISPs') and payment initiation service providers ('PISPs').

- The GDPR is about establishing a framework to ensure that entities holding personal data keep that personal data safe and secure/protected against undue sharing with other parties (at least without a lawful basis to be found in the GDPR).

So it is no surprise that as part of PSD2 projects that Bird & Bird have been handling for clients, questions have arisen such as: "If we comply with the PSD2, surely we will breach the GDPR!?," and vice versa as part of GDPR projects for payments companies.

Below, we address some of the most burning issues that we have encountered over the last year or so (but this article by no means seeks to be exhaustive)[1]. We will address in turn:

- whether the PSD2 is *lex specialis* versus the GDPR;
- the concept of 'explicit consent' under the PSD2 and the GDPR;
- TPPs having access to accounts that do not qualify as 'payment accounts' under the PSD2 and the interplay with the GDPR;
- the processing of 'silent parties' data under the PSD2 and the GDPR;
- TPPs using data for other purposes than those set out in the PSD2, and the link with the GDPR; and
- the interplay between incident notification requirements under the GDPR and the PSD2.

Most of the issues at the interplay of the PSD2 and the GDPR can, and have been resolved, in such a way as to ensure compliance with both the PSD2 and the GDPR. However, there are outstanding issues, as we will indicate below.

Are the PSD2 provisions on data protection *lex specialis* versus the GDPR?

Article 94 of the PSD2 deals with data protection. In particular, Article 94(2) of the PSD2 provides that:

'Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.'

This begs the question of whether Article 94(2) of the PSD2 is *lex specialis* versus the GDPR, meaning that the legal basis for a payment service provider ('PSP') to process personal data could only be explicit consent, as opposed to any other legal basis contained under the GDPR (e.g. compliance with legal obligation, legitimate interests, contractual necessity, etc.). If Article 94(2) of the PSD2 is not *lex specialis* versus the GDPR, would it mean that a PSP would have to comply with the requirement of Article 94(2) of the PSD2 and the GDPR?

There has been movement on this issue:

- On 20 December 2017, the Dutch data protection authority ('AP'), in a letter addressed to the Dutch Minister of Finance, Wopke Hoekstra, stated that "[the] PSD2 constitutes a *lex specialis* [...] for the processing of personal data for payment services[2]."
- Since then, the European Commission ('the Commission') indicated, during various conferences, that Article 94 of the PSD2 is not *lex specialis* versus the GDPR.
- On 5 July 2018, the European Data Protection Board ('EDPB'), in a letter sent to Dutch MEP, Sophie in't Veld, also (implicitly) expressed the view that Article 94 of the PSD2 is not *lex specialis* versus the GDPR[3].
- On 19 October 2018, the AP issued a further publication on the interplay of the PSD2 and the GDPR, and this time took the view that the PSD2 is not *lex specialis* versus the GDPR[4].

Therefore, there now seems to a general consensus that Article 94 of the PSD2 is not *lex specialis* versus the GDPR, and therefore a PSP has to comply with both Article 94 of the PSD2 (including the explicit consent requirement) and the GDPR provisions requiring an entity processing personal data to have a lawful basis (e.g. GDPR consent, compliance with legal obligation, legitimate interests, contractual necessity, etc.).

Is there a difference between Article 94 PSD2 explicit consent, and GDPR (explicit) consent?

As mentioned above, Article 94 of the PSD2 provides that a PSP should obtain the 'explicit consent' of the payment service user ('PSU') in order to be able to access, process and retain their personal data. We have received a lot of questions on what that explicit consent is. Is it GDPR consent? Or is it specific PSD2 consent that should not be read as GDPR consent?

Consent under the GDPR is probably one of the most complicated lawful bases to implement. Indeed, GDPR consent shall be freely given, specific, informed and unambiguous. Also, it shall be given by a clear affirmative act. This means that silence, pre-ticked boxes or inactivity do not constitute valid consent under the GDPR. Therefore, under the GDPR:

- consent must be granular for each purpose of processing and must be presented separately;
- services cannot be made conditional on consent for unrelated processing (no bundling); and
- PSUs must be able to withdraw their consent as easily as it is given.

'Explicit consent' under the GDPR is separate from 'consent.' Although there is no definition of explicit consent under the GDPR, according to the UK Information Commissioner's Office ('ICO'), "the key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written)[5]." Therefore, in order to obtain valid GDPR explicit consent, the PSP would have to provide the PSU with a written express statement of consent that the PSU should have to sign or accept. GDPR 'explicit consent' is therefore much more challenging to obtain than obtaining regular GDPR 'consent,' (which is already complicated enough to obtain).

Explicit consent under the GDPR is only required as a lawful basis to collect, process and disclose special categories of personal data[6]. Therefore, GDPR explicit consent is not required to process payments or transaction data.

Under the GDPR, a PSP would not need even the consent of the PSUs to access, process and retain their personal data; it could easily rely on another lawful basis, such as contractual necessity (Article 6(1)(b) of the GDPR).

Therefore, taking all the above into consideration (i.e. the requirements that valid consent under the GDPR shall meet, the fact that payments data do not require explicit consent under the GDPR, and the fact that entities can rely on another lawful basis to process this kind of data), it seems that the explicit consent required under the PSD2 should not be read as GDPR (explicit) consent.

This view is shared by the EDPB, which expressed the view that the explicit consent referred to under Article 94(2) of the PSD2 is contractual consent. According to the EDPB:

"Article 94 (2) of the PSD2 should be interpreted, on the one hand, in coherence with the applicable data protection legal framework and, on the other hand, in a way that preserves its useful effect. This implies that Article 94 (2) of the PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. Such

clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject. The concept of explicit consent under Article 94 (2) of the PSD2 is therefore an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR[7]."

The EDPB also considers that the lawful basis to process personal data under the GDPR would be the contractual necessity (not GDPR consent).

Consequently, and from a practical perspective, when implementing the PSD2, PSPs will have to build an explicit consent mechanism aligned with the PSD2, but not with the GDPR. As far as GDPR is concerned, they will have to rely on another lawful basis (namely, contractual necessity) to process data from a GDPR perspective. This will clearly simplify the user experience, while ensuring consistency with both the PSD2 and the GDPR.

The ASPSP gives TPPs access to personal data without having seen the PSU's explicit consent - does this place the ASPSP in breach of the GDPR?

Under the PSD2, ASPSPs have to give access to payments accounts as soon as a TPP contacts the ASPSP claiming to have received explicit consent from the PSU to access the payment account(s). The ASPSP is not entitled to receive a copy of the explicit consent (allegedly) collected by the TPP, or to seek a confirmation or second explicit consent from the PSU[8]. Therefore, an ASPSP will grant access to the PSU's payment account(s) without having seen the explicit consent (allegedly) given by the PSU to the TPP. Does that put the ASPSP in violation of the GDPR?

In our view, no. The GDPR provides for various lawful bases for the ASPSP to lawfully process the data, i.e. in this case, make the data available to the TPP[9]. Consent from the PSU is one of them, but is not the only one. In this case, we believe that the ASPSP would provide the data to the TPP in compliance with the GDPR because under Article 6(1)(c) of the GDPR, the 'processing is necessary for compliance with a legal obligation under EU law or the laws of a Member State to which the controller is subject.'

It is our understanding that the Commission is in agreement with us on this issue.

'Silent party' data - is there a GDPR issue?

When a PSU gives their explicit consent for a TPP to access their payment account(s), pursuant to Article 36 (1)(a) of the regulatory technical standards ('RTS') on strong consumer authentication ('SCA') and common and secure communication ('CSC'), the ASPSP:

'shall provide [AISPs] with the same information from designated payment accounts and associated payment transactions made available to the PSU when directly requesting access to the account information, provided that this information does not include sensitive payment data.'

The AISP will therefore not only have access to (personal) data related to the PSU, but also (personal) data related to third parties, so-called 'silent parties' (e.g. name and/or address and/or international bank account number of persons to whom the PSU recently transferred money, or from whom the PSU recently received money). Two questions arise from this situation:

- Is the ASPSP in breach of the GDPR by providing personal data related to silent parties to TPPs?
- Is the TPP in breach of the GDPR by accessing personal data from silent parties and processing that data in order to provide a service to the PSU?

In our view, the ASPSP is not in breach of the GDPR by providing silent party data to the TPP. It is providing the silent party data to the TPP in order to comply with its legal obligation, in line with Article 6(1)(c) of the GDPR[10].

As regards the TPP, we also believe that it can process the silent party data without breaching the GDPR because under Article 6(1)(f) the 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party [...].' The EDPB shares this opinion, and considers that:

"a lawful basis for the processing of these silent party data by PSIPs or AISPs - in the context of payment and account services under the PSD2 - could be the legitimate interest of a controller or a third party ex Article 6 (l)(f) to perform the contract with the service user. This means that the legitimate interest of the controller is limited and determined by the reasonable expectations of data subjects."

However, it is important to note that TPPs cannot apply the legitimate interest basis automatically to process personal data. The GDPR requires that all entities making use of this legal basis carry a balancing test to assess whether their legitimate interest effectively overrides the individuals' rights. Entities shall therefore be able to demonstrate that they have an actual legitimate interest. To do this, they will need to take into consideration a number of factors, such as the kind of data collected, the context, the circumstances, the risk for the individuals, etc.

Can a TPP 'recycle' the data to provide other services to the PSU?

Article 66(3)(g) of the PSD2 reads as follows:

'The [PISP] shall [...] not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer.'

This suggests that a PISP could only use the data collected as a PISP to provide a payment information service to the PSU, and nothing else, even with the GDPR consent from the PSU to re-use that data to provide other services to the PSU.

Article 67(2)(f) of the PSD2 provides that:

'The [AISP] shall [...] not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, **in accordance with data protection rules** [emphasis added].'

The meaning of the words that we emphasised is unclear. Does this mean that, with the PSU's GDPR consent, could the AISP re-use the data it collected, acting as AISP, in order to provide other services to the PSU (e.g. a mortgage comparison service)?

This is one of the burning issues at the interplay of the PSD2 and the GDPR and, to our knowledge, no authority (whether the Commission, the European Banking Authority ('EBA'), national financial services or data protection authorities) has expressed an official view on this key issue[11].

We are however aware that the Hungarian Central Bank ('MNB'), for example, has expressed the unofficial view that an AISP cannot re-use the data collected as an AISP to provide other services to the PSU, even with the PSU's GDPR consent.

It is to be noted that in some EU countries, the words that we emphasised above were not incorporated within the national law transposition of the PSD2, which makes the situation even more complicated, and leads to potential different answers in different EU Member States[12].

In Hungary, the emphasised words were incorporated within national legislation under Article 81(c) of Act 126 of 2018 on the harmonization related modification of certain finance related laws amending the Hungarian Payment Services Act (Act 85 of 2009), and we therefore respectfully disagree with the position unofficially adopted by the MNB (i.e., we believe that with freely given, specific and informed consent from the PSU, the AISP should be able to use the data for further purposes, i.e., for provision of additional services to the PSU):

- The position of the MNB seems to simply ignore/give no meaning to the emphasised words, and therefore treat AISPs like PISPs (in relation to which the emphasised words do not appear). Surely the emphasised words should be given some meaning?
- One of the possible reasons why the MNB took this view is because it considered only the consumer protection aspects of this question, but did not consider the principle of informational self-determination under which data subjects (in this case PSUs) can control processing of their personal data. Indeed, pursuant to the GDPR, the personal data belongs to the data subject. Therefore, in our opinion, if a data subject is content with an AISP using the data to provide them with other services than the account information service ('AIS'), this is compliant with the GDPR, and the PSD2 should not make this illegal. The first argument is supported by the Article 29 Working Party ('WP29') Guidelines on Consent under the GDPR ('the Consent Guidelines')[13]. On p.9 of the Consent Guidelines, example 6 addresses a scenario where a bank requests its customers to consent to third parties using their payment details for direct marketing purposes. The WP29 concluded that this is possible, as long as the consent is valid and freely given. Whether the consent of the PSU for this further data processing activity is valid, i.e. whether it is freely given, specific, informed and unambiguous, is a matter of fact which should be considered based on the offering of the AIS. We believe that a categorical "no" to this question is not the right answer.
- If an AISP was not able to use the data collected to provide the AIS in order to provide other (non-AIS) services to the PSU, while other market players (e.g. mortgage comparators), sometimes unregulated, would be allowed to use that same data to provide other services to the PSU, this would create an unfair distortion of competition between (regulated) AISPs and those (sometimes unregulated) market players.

We are therefore of the view that, as long as the PSU has given consent to the AIS that meets the conditions of the GDPR, an AISP should be allowed to use the data used to provide the AIS in order to provide other services to the PSU.

Access to data from accounts that are not payment accounts

The PSD2 regime is about access by TPPs to payment accounts (that are accessible online).

Payment accounts are defined under Article 4(12) of the PSD2 as 'an account held in the name of one or more payment service users which is used for the execution of payment transactions.'

In a judgment dated 4 October 2018, the Court of Justice of the European Union ruled that:

"31. [...] the possibility of making payment transactions to a third party from an account or of benefiting from such transactions carried out by a third party is a defining feature of the concept of 'payment account.'

32. An account from which such payment transactions cannot be made directly, but for which use of an intermediary account is necessary, cannot therefore be regarded as being a 'payment account' [...][14]."

This judgment confirmed what should have been obvious to all (including to the EU legislator), but apparently was somehow not, which is that most savings accounts in the EU do not qualify as payment accounts, and therefore the PSD2 access to payment accounts regime is essentially granting TPPs the right to access current accounts, but nothing more.

However, in order for AISPs to be successful (which is the objective of the PSD2), AISPs need to have access to accounts other than just current accounts, and at a minimum also need to have access to savings accounts. Therefore, AISPs will find themselves accessing different accounts in different ways:

Current accounts

TPPs will access current accounts under the heavily regulated, and hopefully secure, regime prescribed under the PSD2 and the RTS on SCA and CSC (i.e. dedicated or non-dedicated interfaces in the case of a dedicated interface a contingency mechanism, or fallback needs to be provided to TPPs, etc).

Savings accounts and other non-payment accounts

AISPs have no legal right of access to non-payment accounts under the PSD2 and the RTS on SCA and CSC. This begs the question of whether AISPs can access those accounts (e.g. via the screen scraping or reverse engineering technologies that have typically been used by TPPs to access all accounts pre-PSD2) or not.

Our view is that since accessing those accounts under the Payment Services Directive (Directive (EU) 2007/64/EC) (PSD1) was considered to be legal, there is no reason to consider that continuing to access those accounts based on those technologies would suddenly have become illegal.

We believe that should an ASPSP try to restrict access to those non-payment accounts, it may potentially face legal issues under competition law.

In addition, could it be argued that a PSU giving their 'explicit consent' to an AISP to access their non-payment accounts would be nothing else but the PSU exercising their right to data portability, which is regulated under Article 20 of the GDPR?

- In this sense, following the WP29 Guidelines on the Right to Data Portability[15], we think that a request to access non-payments accounts should not be treated as a data portability right under the GDPR, unless the PSU clearly requests this formally[16].
- It is also important to note that the right to data portability is not an 'absolute' right that can be requested in all circumstances, and over any kind of data. In this sense, data portability is limited to data concerning the PSU that they have provided to the data controller, and the processing operations must be based either on consent or contractual necessity.

Incident notification requirements

In a previous article in *Payments & Fintech Lawyer*, available for download here, we analysed the major incident notification requirements under the PSD2. We therefore do not address them in detail again here, and focus more instead on the GDPR notification requirements, and the differences between the PSD2 and GDPR notification requirements.

It is important to note that, as indicated in the WP29 Opinion 03/2014 on Personal Data Breach Notification[17], the 'breach' referred to under the GDPR, while being a type of security incident, only applies to the extent that it affects personal data. Therefore, although all personal data breaches are incidents, not all security incidents are necessarily personal data breaches.

Entities subject to the GDPR and the PSD2 will have to follow two notification processes in case they suffer a major security incident involving personal data. In such cases, it is crucial that both notification processes are coordinated and consistent. For the sake of clarity, we have summarised in the table below the requirements under the GDPR and the PSD2:

	Data Breach - GDPR	**Security Incidents - PSD2**
Definition	The GDPR describes personal data breaches as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'	The Guidelines on major incident reporting under the PSD2 describe a security incident as 'a singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services[18].'
Types	1. **Confidentiality breach**: where there is an unauthorised or accidental disclosure of, or access to, personal data; 2. **Integrity breach**: where there is an unauthorised or accidental alteration of personal data; and 3. **Availability breach**: where there is an accidental or unauthorised loss of access to, or destruction of, personal data.	1. **Operational**: an incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services[19]. 2. **Security**: unauthorised access, use, disclosure, disruption, modification or destruction of the PSP's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services. This may happen when, among other things, the PSP experiences cyber attacks, inadequate design or implementation of security policies, or inadequate physical security.

Competent authority	The competent authority in the home Member State of the data processing[20].	Firstly, to the competent authority in the home Member State of the PSP. Secondly, to the competent authority in charge of enforcing the PSD2[21]. At the end, competent authorities should always provide the EBA and the European Central Bank with all reports received from (or on behalf of) PSPs affected by a major operational or security incident (i.e. initial, intermediate and final reports)[22].
Timeline to notify	A maximum of 72 hours after having become aware of the breach[23].	• **Initial Report**[24]: PSPs should send the initial report to the competent authority within four hours from the moment the major operational or security incident was first detected. PSPs should also submit an initial report to the competent authority when a previously non-major incident becomes a major incident. In this particular case, PSPs should send the initial report immediately after the change of status is identified. • **Intermediate Report**[25]: PSPs should submit intermediate reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report. Furthermore, PSPs should indicate in each reports the date for the next update, which should be as soon as possible and under no circumstances going beyond three business days. • **Final Report**[26]: PSPs should deliver the final report to the competent authority within a maximum of two weeks after business is deemed to be back to normal.
Information to report	The data controller should elaborate a single report by which the data breach will be	**Initial Report**[28]: • the type of report;

	communicated and which will contain at least the following aspects[27]: • a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned; • the name and contact details of the data protection officer, or other contact point where more information can be obtained; • the likely consequences of the personal data breach; and • the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	• the affected PSP (e.g. PSP name, PSP authorisation number, home country, telephone); • the reporting entity, this section should be completed if a third party fulfils the reporting obligations on behalf of the affected PSP; • the date and time of detection of the incident; • the date and time of beginning of the incident; • the short and general description of the incident; and • the estimated time for the next update (interim or final report). **Intermediate Report**[29]: • a more detailed description of the incident; • the date and time of beginning of the incident; • the incident status; • the date and time when the incident was restored or is expected to be restored; • the overall impact; • the transactions affected; • the PSUs affected; • service downtime; • the economic impact; • the highest level of internal escalation; • other PSPs or relevant infrastructures potentially affected; • reputational impact, • an incident description (e.g. type of Incident, cause of incident); • the incident impact (e.g. building affected, payment services affected, functional areas affected, systems and components affected, staff affected); and

		• incident mitigation (e.g. actions/measures, business continuity plan). **Final Report**[30]: • an update of the information from the intermediate report; • the date and time of closing the incident; • whether or not the original controls are back in place; • the root cause; • the main corrective actions/measures taken or planned to prevent the incident from happening again in the future; • whether the incident has been shared with other PSPs for information purposes; and • legal action taken against the PSP. Should the PSP be able to provide all the information required in the final report within the four hour window since the incident was detected, they should aim to submit in their initial report the information related to initial, last intermediate and final reports.

Conclusion

As we hope is clear from the above, there were tensions between the PSD2 and the GDPR, but they can be reconciled so that PSPs are able to comply with both the PSD2 and the GDPR at the same time.

One of the most burning issues at the interplay of both legislations is the delineation of the activities that AISPs are allowed to perform with the data that they collected while acting as AISPs (can they only use that data to provide an AIS, or also to provide other services?). We trust that the EC, the EBA and/or the EDPB will soon publish on this topic in order to ensure legal certainty on this key issue. If the answer were to be that AISPs cannot use the data for other purposes that account information service even with the PSU's consent, and/or that access by TPPs to non-payments is not guaranteed, the call for having a 'PSD3' as soon as possible would only get stronger.

Scott McInnes Partner
scott.mcinnes@twobirds.com
Lupe Sampedro Partner Bird & Bird LLP

lupe.sampedro@twobirds.com
Bird & Bird LLP, Brussels, London & Madrid

---

1. Note that we have identified over potential contractions between payments regulation and data protection legislation. For example a payment service provider that would like to invoke the benefit of the Transaction Risk Analysis ('TRA') exemption to SCA is required 'as a result of performing a real time risk analysis have not identified any [...] abnormal location of the payer,' under Article 18(2)(c) of the regulatory technical standards on strong consumer authentication and common and secure communication. However, pursuant to the draft ePrivacy Regulation that is currently in the EU legislative adoption process, it is possible that the payment service provider would be required to obtain the consent from the payment service user – which would seriously undermine the possibility for a payment service provider to make use of the TRA exemption to strong consumer authentication.
2. English translation of the letter available at: https://www.twobirds.com/~/media/pdfs/dutch-dpa-letter-to-dutch-minstry-of-finance.pdf?la=en
3. Letter available at: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en
4. English translation available at: https://www.twobirds.com/en/news/articles/2018/netherlands/further-guidance-on-explicit-consent-under-psd-by-dutch-dpa
5. Document available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
6. Under Article 9(1) of the GDPR, special categories of data are: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data processed for the purpose of uniquely identifying an individual, data concerning health, or data concerning an individual's sex life or sexual orientation.
7. Letter available at: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en
8. Although, *de facto*, if the ASPSP gets to perform a strong customer authentication of the PSU, this will give some practice assurance to the ASPSP that the PSU is content with TPP accessing his payment account(s), as otherwise the PSU would not apply strong consumer authentication in that operation.
9. In the case of an AISP, the regulatory technical standards states that the AISP would get the same data as the users when they log into their payment accounts directly with their ASPSPs. With regard to PISPs, there is still uncertainty as to what data a PISP should see.
10. This is also begs the question of what the legal basis is for an ASPSP to process the silent party data for the purposes of providing services to the PSU (without any TPP being involved). Arguably, legitimate interests (and/or perhaps compliance with legal obligation, e.g. anti-money laundering legislation).
11. The EDPB has commented on a similar issue in relation to silent party data (whose data is processed on the basis of legitimate interests since the data subject does not have a relationship with the TPP), but has not commented on the issue as regards the PSU's data (which is processed on the basis of consent since the PSU has a relationship with the TPP). As regards silent party data, the EDPB stated: "with regard to further processing of silent party data on the basis of legitimate interest, the EDPB is of the opinion that these data cannot be used for a purpose other than that for which the personal data have been collected, also given the restrictions on processing set out in Article 66 (3)(g) and Article 67 (2)(f) of the PSD2 and that data subjects do not reasonably expect any further processing."
12. For example France, Germany, Denmark, Sweden, etc., did not include the words that we emphasised within their national legislation.
13. Document available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
14. Judgment of the Court (Fifth Chamber), 4 October 2018, Case C-191/17. For more details on this judgment, see the Bird & Bird client alert at: https://www.twobirds.com/en/news/articles/2018/global/the-cjeu-provides-clarity-on-the-definition-of-a-payment-account

15. Guidelines available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
16. The WP29 includes the following example in its Guidelines on the Right to Data Portability: 'if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in [the PSD2] such access should be granted according to the provisions of this directive.'
17. Document available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
18. EBA Guidelines on Major Incident Reporting Under PSD2, p.18, available at: https://eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf
19. Ibid, p.41.
20. Article 33(1) of the GDPR.
21. Article 96(1) of the PSD2.
22. Article 96(2) of the PSD2.
23. Article 33(1) of the GDPR.
24. EBA Guidelines on Major Incident Reporting Under PSD2, p.25.
25. Ibid, p.25–26.
26. Ibid, p.26.
27. Article 33(3) of the GDPR.
28. EBA Guidelines on Major Incident Reporting Under PSD2, Annex 1 p.36-38.
29. Ibid, p.38-44.
30. Ibid, p.44.

RELATED CONTENT

OPINION

USA: Musical.ly settlement indicates "FTC is willing to push beyond its past actions"

NEWS POST

Netherlands: AP issues guidelines on tracking cookies

NEWS POST

Spain: AEPD publishes study on Android applications information flows

LEGAL RESEARCH

Notice No.: CMG-N02 (21 June 2013) (as revised)

LEGAL RESEARCH

MAS Notice 644 (21 June 2013)