ERHVERVSMINISTERIET

NOTAT

22. juni 2022
2022 - 8705
nicsch

Public consultation on the review of the revised payment services Directive (PSD2) and on open finance

Payment methods

Question 1. How do you usually pay for goods and services?
For each payment method, please indicate how often you use it

a) In a physical shop:
   - Cash
   - Payment card (debit or credit)
   - Digital wallet on mobile phone
   - Other payment solutions

   1 (preferred option) 2 (sometimes) 3 (never) Don't know – No opinion – Not applicable

Reply: Not applicable

Please specify to what other payment solution(s) you refer in your answer to question 1 a):
   - Comment box

b) Online:
   - Payment card (debit or credit)
   - Digital wallet on mobile phone
   - Digital wallet on PC or laptop
   - Bank transfer
   - Other payment solutions

   1 (preferred option) 2 (sometimes) 3 (never) Don't know – No opinion – Not applicable

Reply: Not applicable

Please specify to what other payment solution(s) you refer in your answer to question 1 b):
   - Comment box

Question 2. The Payment Services Directive aims to promote innovative internet-based and mobile payment services.

Do you think that the payments market is innovative enough?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Yes

Question 2.1 Please explain why you don't think the payments market is innovative enough:

- Comment box

Reply:
After PSD2 the market has developed several innovative solutions through third party payment service providers (TPPs) that has been driven in large part by the regulation. However, there is a risk that innovation will stall if the regulation is too detailed and complex.

Regulation should be principle-based rather than developing detailed regulatory requirements to ensure that the framework does not stall regulation and confines to market participants to predefined solutions.

This is a general thread that follows in our answers below, e.g. with regards to security solutions.

With regards to non-TPP payment institutions further initiatives can be considered to support the operational independence of such entities. To this end, it is important to review art. 36 of PSD2 on Access to accounts maintained with a credit institution to ensure a harmonised approach across the EU and provide clarity on the interplay with AML-rules. Also the Settlement Finality Directive should be revised to allow payment institutions and electronic money institutions to participate directly in the settlement and clearing systems.

Finally, a revision of art. 35 of PSD2 on Access to payment systems is needed. This provision grants PSP (e.g. card acquirers) the right to access payment systems (e.g. card networks) to provide payments services in order to increase competition, e.g. among acquirers within a card network. This is especially relevant within smaller national card schemes that are often dominated by a single acquirer. The current wording of the provision has in practice proved to be too vague to provide supervisors with the proper legal basis to enforce it in accordance with the intention. Inspiration could be drawn from art. 36 to ensure a more operational wording.

In recent years, have entered the market. Many are not banks, and **new payment service providers** they include big tech companies (i.e. large online platforms offering search engines, social networking services and more).

Question 3.1 Do you believe that you have a larger choice of payment services than you did 5 years ago?

- Yes
- No, I have the same choice as before
- No, I have less choice
- Don't know / no opinion / not applicable

Reply: Not applicable

Question 3.2 What do you think about new companies, including big tech companies, entering the payments market?

- Comment box

Reply:
Though it does not seem to have reached its full potential yet, the entrance of new players, especially third party payment services providers, has led to more competition and innovation in the market, e.g. with regards to bill payments and use of data in online banking environments.

Big techs can provide the market with further competion and lead better and cheaper services for consumers. However, we should be careful to avoid that market concentration with big techs lead to worse outcomes.

Before any initiative to further expand data-sharing requirements developed, it should thoroughly considered how such initiatives will impact a level playing field between different market players and avoid concentration risks.

To use these services, payment service providers need access to your payment account(s) data, which requires your consent. There are two kinds of providers

- **Account information services providers (AISP)**: these access data from your online accessible payment account(s) and consolidate these data to, for example, help you manage your finances
- **Payment initiation services providers (PISP)**: these provide an online service that accesses your payment account to transfer funds on your behalf with your consent and authentication. For example, you could have payment accounts from different banks together in a PISP app on your phone and transfer funds from any of those payment accounts directly from the app

AISPs and PISPs do not actually handle your funds. Once they have your consent, AISPs get access to your transaction history, and PISPs facilitate the payment, but they never come into possession of your funds.

Question 3.3 Do you use AISPs and/or PISPs?

- I only use AISP(s)
- I only use PISP(s)
- I use both AISPs and PISPs
- I don't use any of them
- Don’t know / no opinion / not applicable

Reply: Not applicable

Question 3.4 If you do not use AISPs and/or PISPs, what are your reasons for this?

- I don’t need their services
- I don’t trust those providers
- I don’t want to share my data with other companies besides my own bank
- I did not know these providers exist
- Other

Reply: Other

Please specify to what other reason(s) you refer in your answer to question 3.4:

- Comment box

Reply:
While we recognize that AISPs and PISPs have brought about increased innovation and competition in the market as also mentioned in answers to previous questions, going forward, it is important to consider how personal data is properly protected and for what purposes it is processed.

It should be considered whether the user is fully aware of the purposes data are used for and what entities process the data. This is especially relevant when data is retrieved by one entity (the entity gathering the consent from the user) and processed by another entity without the data (in raw or processed form) being presented to the user.

Further is should be noted that payments data and other personal data can be used for price discrimination or lead financiel inclusion. An increased access to data should be accompanied with thorough consideration as to how such issues are tackled.

Digital payments

Question 4. Do you make digital payments?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Not applicable

An important objective of the Payment Services Directive was to make digital payments (non-cash payments using electronic payment instruments, e.g. payment cards, mobile phones, etc.) and online banking safer and easier for consumers.

Question 4.1 Based on your experience with digital payments over the last 5 years, please indicate to what extent you agree with the following statements:

- Making digital payments has become easier
  Reply: 2
- It has become easier to make digital payments to other EU countries (e.g. when buying from an online shop in another EU country)
  Reply: 2
- It has become easier to make digital payments to non-EU countries (e.g. when buying from an online shop in a non-EU country)
  Reply: 3
- It has become easier to transfer money to other EU countries
  Reply: 2
- It has become easier to transfer money to non-EU countries
  Reply: 3

1 (strongly agree) 2 (somewhat agree) 3 (neutral) 4 (somewhat disagree) 5 (strongly disagree) Don't know – No opinion – Not applicable

The Payment Services Directive includes measures to protect consumers. Some examples are described below (please note that the below is not an exhaustive list)

- Transparency: before and after transactions have been executed, payment service providers must inform users about all fees payable, when the transaction will be completed, etc.
- Rights and obligations: for some unauthorised payment transactions, the Directive has limited the liability of the payer, for example, when a payment card is lost
- Fraud prevention: PSD2 introduced strong customer authentication (SCA, see explanation below) for making payment transactions or giving access to payment accounts

The following questions ask your opinion on consumer protection and the Payment Services Directive.

Question 4.2 Please indicate to what extent you agree with the following statements about information and fees:

- Before paying (either online or in a physical shop), I know if I will have to pay a fee in addition to the price of the product(s) or service(s) purchased
- The cost of any fees is always clear
- If a payment includes a currency conversion (e.g. from euro to Swedish Krona), it is always clear what exchange rate will be applied
- When charged with fees for ATM cash withdrawals, it is always clear what these fees are
- When withdrawing cash abroad at an ATM in another currency, it is always clear what exchange rate will be applied
- The information I receive before I make a payment is sufficient

1 (strongly agree) 2 (somewhat agree) 3 (neutral) 4 (somewhat disagree) 5 (strongly disagree) Don't know – No opinion – Not applicable

Reply: Not applicable

Question 4.2.1 If you find that the information provided to you during a payment transaction or cash withdrawal is not always clear, please explain what is not clear?

- Comment box

Reply:
In general, it should be considered whether the provided information is in practice adjusted to the needs of the avarage consumer and puts the consumer in a position to act if needed. Information overload should be avoided and behavioral insights taken into consideration when developing requirements related to consumer information.

Further, it should be noted that the provided information does not always provide the user with knowledge of underlying og indirect costs. In this regard, the current prohibition on surcharges (PSD2 art. 62,4) can lead the user to make use of payment instruments that can lead to increased prices for other products or services. We would suggest that the surcharging ban is evaluated on this background.

Question 4.2.2 Do you require additional information before making a payment?

- Yes
- No

- Don’t know / no opinion / not applicable

Reply: Not applicable

Please explain what additional information you need before making a payment:

- Comment box

To make payment transactions more secure and prevent fraud further, the Payment Services Directive introduced strong customer authentication (SCA or ‘2-factor authentication’). This requires authentication through a combination of two of the following three factors: ‘something I possess’ (e.g. card, mobile phone), ‘something I know’ (e.g. PIN), or ‘something I am’ (e.g. fingerprints).

Making a payment, either in a physical shop or online, usually involves SCA (except in certain circumstances, e.g. low-value contactless payments). SCA can be done using a mobile phone or through other means, such as card reader or a code-generating device.

Question 4.3 What is your opinion about confirming your payment with SCA?

a) When buying something in a physical shop:

- It is easy, and I have no problem with it
- It is cumbersome, but I accept it because it protects me against fraudsters
- It is cumbersome, and I do not see the point of it
- Other
- Don’t know / no opinion / not applicable

Reply: Not applicable

Please specify to what is your opinion about confirming your payment with SCA when buying something in a physical shop:

- Comment box

Reply:
In general, SCA in a physical environment is well known with merchants and consumers and works relatively seamlessly. However, the exemption for contactless payments should be differentiated between countries to ensure that limits are fit for the price levels of different Member States.

b) When buying something online:

- It is easy, and I have no problem with it

- It is cumbersome, but I accept it because it protects me against fraudsters
- It is cumbersome, and I do not see the point of it
- Other
- Don't know / no opinion / not applicable

Please specify to what is your opinion about confirming your payment with SCA when buying something online:
- Comment box

Reply:
The application of strong customer authentication (SCA) has lead to a significant decrease in fraud cases for online payments and from that point of view this initiative can be considered a success. However, it should also be considered whether the requirement has been efficient when taking into account the costs in terms of inconvenience for users and not least lack of financial inclusion for vulnerable and non-tech savvy citizens.

While the use of electronic payments can be substituted by cash or paper-check payments in some Member States, citizens in the most digitized Member States increasingly have to rely solely on electronic payments. We would therefor urge the Commission to consider how security requirement can be made more flexible to ensure that payment service providers can better accommodate all user groups.

Payment service providers are required to implement SCA and can decide how to implement it. They usually enable SCA via a mobile phone app and/or another specific device.

Question 4.3.1 Besides payments made on mobile phones, do you think payment service providers should be required to offer SCA solutions other than through mobile phones?

- Yes
- No
- Don't know / no opinion / not applicable

Reply:
In general, regulation should not mandate specifc technological solutions, however a general requirement to ensure that SCA solutions cater to all user groups could be considered.

Should a general requirement to ensure that security solutions are fit for all user groups be introduced, we find it very important that is complemented with the introduction of more flexibility in the general requirement, as sketched out above, to ensure that payment service providers have the room to meet the requirement without stalling innovation.

Question 4.3.2 Do you believe payment service providers should put in place more security measures?

- Yes
- No
- Don’t know / no opinion / not applicable

Reply: Yes

Please explain your answer to question 4.3.2 and include any suggestions:

- Comment box

Reply:
Our experience is that fraud is increasingly carried out using social engineering so further security measures directly involving the PSU would not be warranted. However, increased reliance on transaction monitoring, including behavioral biometrics, could be a solution. Transaction monitoring is already mandated in the RTS on CSC and SCA, but could be introduced directly in the directive instead.

Since the COVID-19 pandemic, the number of contactless payments has increased significantly. The maximum amount for contactless payment transactions without SCA was increased to EUR 50 by payment service providers in most countries.

Question 4.4.1 What do you think about the maximum amount for a contactlesspayment (without SCA)?

If the euro is not the main currency in your country of residence, please convert EUR 50 to your local currency and select an answer:

- The EUR 50 limit should remain
- The limit should be lower than EUR 50
- The limit should be higher than EUR 50
- I should be able to set my own limit
- Other
- Don’t know / no opinion / not applicable

Reply: The limit should be higher than EUR 50

Please specify to what other view(s) you have on the maximum amount for a contactless payment (without SCA):

- Comment box

Reply:
The exemption for contactless payments should be differentiated between countries, potentially as a Member State option, to ensure that limits are fit for the price levels of different Member States.

Since the PSUs PSP is liable for any fraud occuring without the use of SCA, the PSP should be able to set the maximum limit. If the PSP wishes, it can let the PSU set its own limit within that maximum.

There is also a limit to the cumulative value of contactless payments, which differ by country. For example, in Germany, one must enter a PIN every three to five transactions or when a total of EUR 150 has been spent. In Czechia, a PIN is required for every third consecutive transaction.

Question 4.4.2 What is your opinion about this cumulative limit for contactless payments (without SCA)? Please give one answer for the value limit and one for the payments limit.

If the euro is not the main currency in your country of residence, please convert EUR 50 to your local currency and select an answer for 'Value in euro':

a) Value in euro:
   - The limit should be lower than EUR 150
   - The limit should be higher than EUR 150
   - I should be able to set my own limit (including EUR 0)
   - Other

   Reply: Other

   Please specify to what other view(s) you have on the value limit for contactless payments (without SCA):
   - Comment box

   Reply:
   The exemption for contactless payments should be differentiated between countries to ensure that limits are fit for the price levels of different Member States.

   Since the PSUs PSP is liable for any fraud occuring without the use of SCA, the PSP should be able to set the maximum limit. If the PSP wishes, it can let the PSU set its own limit within that maximum.

b) Number of consecutive payments:
   - This should be less than five consecutive payments
   - This should be more than five consecutive payments

- I should be able to set my own limit (including zero payments)
- Other

Reply: Other

Please specify to what other view(s) you have on the payments limit for contactless payments (without SCA):

- Comment box

Reply:
Since the PSUs PSP is liable for any fraud occuring without the use of SCA, the PSP should be able to set the maximum limit. If the PSP wishes, it can let the PSU set its own limit within that maximum.

Blocking funds
For payments by card, funds can be blocked on your account if the exact final amount unknown at the time of payment. For example, when you are at an unmanned petrol station, you may have to agree to a certain amount of funds to be blocked before you fill up your tank. The blocked amount will then be corrected, and the exact final payment will be processed afterwards.

Question 4.5 Should there be a limit on the amount that can be blocked?

- Yes
- No, no limit is needed
- Other
- Don't know / no opinion / not applicable

Reply: Other

Question 4.5.1 Please explain what should be the limit on the amount that can be blocked:

- Comment box

Reply:
In general, it is a serious consumer problem when higher amounts are blocked and not released in accordance with Article 75(2), making them unable to spend their own money. The Danish Consumer Ombudsman has received complaints from consumers who must wait until the funds are released automatically.

If maximum limits are fixed so that the limits apply in all cases without regard to the specific situation, the blocked amount might be unreasonable high compared to the specific situation/transaction.

For example, consumers driving a motor bike or a moped must have around 80 EUR available on their account to fuel their vehicle – even though a full tank would never amount to that. Further, price levels vary between Member States.

This makes it difficult to introduce general limits, and a possible solution could – at least in some situations – rely on the average price for the purchase in question. However, it is essential that a blocking of funds must be reasoned/justified in each case and fair, also in relation to the amount.

For these reasons, blocking of funds must be reasoned/justified in each case, also in relation to the amount blocked.

Further, it could be considered to introduce requirement regarding the specific situations where funds can be blocked. In certain situations, e.g. fuel stations, blocking can be justified, whereas this might not be the case in other situations.

Question 4.5.1 Please specify what you mean by "other" in your answer to question 4.5:

- Comment box

Reply: See answer to 4.5.1

Fraud

Question 4.6 As a consumer, have you been a victim of payment fraud recently?

- Yes
- No
- Don’t know / no opinion / not applicable

Reply: Not applicable

Question 4.6.1 Please provide details on the payment fraud you have been a victim of:

- Comment box

Question 4.6.2 If you were victim of a fraud did you ask your payment service provider for a refund?

- Yes, and I received a full refund
- Yes, but I only received a partial refund

- Yes, but I did not receive any refund
- Yes, but I requested a refund from another party
- No, I did not request a refund
- Don't know / no opinion / not applicable

Reply: Not applicable

Question 4.6.3 Were you satisfied with the refund process (requesting the refund, communication with your payment service provider, length of the process, etc.)?

- Comment box

Question 4.7 Please indicate to what extent you agree with the following statements about protection and security provided when making digital payments:

- Making digital payments has become more secure
  Reply: 2
- My payments data is adequately protected
  Reply: 2
- Strong customer authentication has helped make digital payments safer and more secure
  Reply: 2
- For digital payments, convenience and speed are more important than security
  Reply: 3

Question 4.7.1 Please explain your answers and include any proposals you may have that further protect digital payments:

- Comment box

Reply:
Our experience is that fraud is increasingly carried out using social engineering so further security measures directly involving the PSU would not be warranted. However, increased reliance on transaction monitoring, including behavioral biometrics, could be a solution. Transaction monitoring is already mandated in the RTS on CSC and SCA, but could be introduced directly in the directive instead.

We find that a more outcome based approach (e.g. setting a maximum fraud level allowed before SCA should be applied) would be a useful approach as such a requirement would be more technologically neutral and provide payment service providers with the largest possible space to innovate and provide consumer friendly solutions, while combatting fraud. An approach with increased reliance on transaction monitoring could be expanded to a

larger section of payments where SCA would only be used for the most high-risk payment could also be considered.

Further, the merit of a one-factor regime in certain cases could also be considered. For large parts of the market the situation went directly from zero-factor to two-factor authentication, leaving us with little insight into whether a one-factor regime could in some cases hit the right balance between security and user friendliness.

Finally, it could also be considered whether the elements of SCA need to belong to different categories, or whether elements could be from the same category.

Considering your responses to the questions above and that the payments market has many new players and technologies (including big tech companies and mobile phone payments):

Question 4.8.1 Do you have specific concerns about the payments market and recent market developments? For instance are there (new) risks that require special attention?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Yes

Please explain your answer to question 4.8.1:

- Comment box

Reply:
Increased use of instant retail payments increases risk of fraud. Further, an instant payments means that the payment is executed before the goods are dispatched. This may put the consumer in worse situation if goods are not delivered. Mitigating measures should be considered.

Regarding the protection of personal data, we refer to the comments under question 3.4 and question 7.

Question 4.8.2 What is your opinion about the level of regulation of the payments market? Is it sufficient or is there too much regulation? Please explain:

- Comment box

Reply:
Over the past decades, financial regulation has become increasingly extensive and complex. This also includes regulation of payment services.

Simultaneously, the interplay with regulation outside financial services has increased this complexity further. Some examples are GDPR and AMLD, where the interplay between open banking rules and GDPR and the interplay between the access for payment institutions to accounts maintained with a credit institution and AMLD has given rise to significant problems when the various sets of rules have been applied in practice. The expected adoption of the regulation on Markets in Crypto Assets (MiCA) will further add to this complexity.

Additionally, the payments market is largely driven by technological developments. It is therefore of utmost importance to ensure that the regulation is in fact technologically neutral and leaves sufficient flexibility for the adoption of new technological solutions in the market.

For these reasons, we find that the guiding principle for the approach to a potential proposal for a PSD3, as well as an open finance framework, should to focus general and principle-based regulation rather than developing detailed regulatory requirements.

Open finance

Open finance refers to a customer allowing their data to be shared or reused by financial institutions and other third-party service providers to access a wider range of innovative services. It could cover different sets of data (business-tobusiness and business-to-consumer data) across a range of financial services (e.g. banking, insurance, investment, pensions). Consumers would be able to grant trusted third-party service providers access to their data, held by financial institutions or other service providers, in a safe and secure way until they decide to revoke their permission. As a result, consumers would have access to better or new services from these third-party service providers, including bettertargeted financial advice, tools to manage their finances, and additional financial services. While the revised Payment Services Directive includes rules on such access for payment accounts (see previous sections of this consultation), no framework currently exists for other financial products.

Question 5. Would you be willing to share the following types of data held by your financial service provider (e.g. bank, insurance company, investment company) with other financial or third-party service providers to get access to new services (e.g. comparing offers, switching providers, financial services tailored to your situation and needs)?

- Savings account data
- Mortgage loan data
- Consumer credit data
- Securities account data
- Pension data

- Insurance data

Yes No Don't know – No opinion – Not applicable

Reply: Not applicable

Please explain your answer to question 5:

- Comment box

Reply:
We refer to our answer under question 3.4 and question 7.

Question 6. Should financial service providers holding your data be obliged to share them with other financial or third-party service providers, provided that you have given your consent?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Not applicable

Question 7. Do you think there are security and/or privacy risks in giving other service providers access to your data?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Yes

Please explain your answer to question 7:

- Comment box

Reply:
Data sharing should be based on a clearly informed basis from the consumers perspective. This is especially relevant when third parties gather data and share it with other parties without the consumer seeing the data before it is shared with further parties.

We have particularly observed some TPPs (mostly for AIS but also PIS) acting as 'API aggregator' that integrate their systems with a wide range of ASPSP's APIs and then provide their own solution to other entity using to access point of the API aggregator to connect to all the ASPSPs connected this service provider.

Such aggregators are used by both regulated TPPs and unregulated entities where the API aggregator runs a license-a-service model. Here the unregulated entity maintains the customer relationship while the API aggregator holds the license and the responsibility to ensure compliance with applicable requirements in PSD2.

This practice is closely related to the Commissions answer to Q&A 2018_4098. If this practice is upheld in a new legislative proposal, it should be considered whether such activities entail specific risks that need to be considered in supervision (and potentially licensing) with regards to data protection and transparency for the consumer.

Question 8. Do you think financial service providers that hold your data always ask for your consent before sharing those data with other financial or third-party service providers?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Not applicable

Question 9. If shared with another financial or third-party service provider, do you think these data are used exclusively for the purposes for which you have agreed?

- Yes
- No
- Don't know / no opinion / not applicable

Reply: Not applicable

Question 9.1 If not, how could this best be ensured?

- Comment box

Reply:
See answer to question 7.

Exchanging data between different service providers could be made more secure by putting in place a dedicated technical infrastructure for that purpose (e.g. a secure application programming interface).

Question 10. If service providers holding data put in place such infrastructure, do you think they should be able to charge a fee to other service providers who access data using this infrastructure?

- Yes
- No

- Don’t know / no opinion / not applicable

Please explain your answer to question 10:

- Comment box

Reply:
In general, we encourage the Commission to continue considering how a fair commercial model for data sharing can be developed to ensure that data providers can cover costs and have an incentive to develop well-functioning access interfaces.

Providing data free of charge limits the financial incentives to provide well-functioning solutions and leads data provide to only deliver the bare minimum to meet regulatory requirements. This leads to a situation where the success of the regulation rests on the ability of legislators and supervisors to define what the market needs - which legislators and supervisors are not very well-position to do. A better outcome might be achieved be establishing a fair commercial model that provides a financial incentive to develop well-functioning solution that meet market demands.