



**EUROPEAN COMMISSION**

DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL  
MARKETS UNION

Horizontal policies  
Retail financial services

## **CONSULTATION DOCUMENT**

### **PUBLIC CONSULTATION ON THE REVIEW OF THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2) AND ON OPEN FINANCE**

#### **Disclaimer**

This document is a working document of the Commission services for consultation and does not prejudice the final decision that the Commission may take.

The views reflected on this consultation paper provide an indication on the approach the Commission services may take but do not constitute a final policy position or a formal proposal by the European Commission.

The responses to this consultation paper will provide important guidance to the Commission when preparing, if considered appropriate, a formal Commission proposal.

You are invited to reply **by 2 August 2022** at the latest to the **online questionnaire** available on the following webpage:

[https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance\\_en](https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance_en)

Please note that in order to ensure a fair and transparent consultation process **only responses received through the online questionnaire will be taken into account and included in the report summarising the responses.**

The views in this consultation paper indicate the Commission's possible approach but do not constitute a final position or a formal proposal. The responses to this consultation will provide important guidance to the Commission in its report on the application and impact of the [revised Payment Services Directive \(PSD2\)](#) and may feed into an impact assessment accompanying a legislative proposal for further revising the PSD2, if considered appropriate. The responses will also help guide the Commission's parallel work on the open finance framework, which is part of the data strategy for Europe.

This consultation follows the normal rules of the European Commission for public consultations. Responses will be published in accordance with the privacy options respondents will have opted for in the online questionnaire.

Responses authorised for publication will be published on the following webpage: [https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance\\_en](https://ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance_en)

Any question on this consultation or issue encountered with the online questionnaire can be raised via email at [fisma-psd2-review@ec.europa.eu](mailto:fisma-psd2-review@ec.europa.eu).

# INTRODUCTION

## Purpose and structure of the consultation

The Commission is launching this public consultation to gather evidence for the PSD2 review and to inform its work on open finance. It targets the public, and no in-depth knowledge of PSD2 or open finance is required. It is available in all official EU languages.

As well as this public consultation, two targeted consultations will be launched: one [targeted consultation on the review of PSD2](#) and the other [targeted consultation on the open finance framework](#). These consultations will have more detailed questions that require specific knowledge of payment services, the PSD2, and data sharing in the financial sector. These targeted consultations are only available in English.

We invite you to respond to

- **this public consultation** if you have little knowledge about the payments industry and the relevant laws
- one or both of the **targeted consultations** if you are a professional stakeholder in the payments industry, e.g. you are a payment institution employee, represent a financial institution members' association, or are knowledgeable about payments

The results of all the consultations will inform the PSD2 review and open finance policy. The results may also serve as input for impact assessments accompanying any possible legislative proposals revising the PSD2 or putting in place an open finance framework.

**In addition to answering to the questions raised in this online survey, you can add any useful documents and/or data (this can be done at the end of this questionnaire).**

**Please give concrete examples in your answers when possible. Where appropriate, please make specific operational suggestions to the questions raised. This will support the review process.**

## Background

The [revised Payment Services Directive \(Directive 2015/2366/EC\)](#) is the basis for payment rules in the EU. The [first Payment Services Directive](#), adopted in 2007, was revised to modernise rules due to increased digitalisation of payments and the emergence of new payment services providers and types of payment services. The Directive became applicable in January 2018, except for some rules on strong customer authentication (SCA) and access to payment accounts, which apply since September 2019.

PSD2 includes rules to

- make it easier and safer to use online payment services
- better protect payment services users against fraud, abuse, and payment problems

- promote innovative payment services
- strengthen the rights of payment services users

PSD2 sets out the conditions under which digital payments are to be executed. For example

- how long it should take for an account to be credited (execution time)
- whether there are fees associated with the transaction
- safety measures to be applied to ensure the security of the payment
- the liability regime in the event of unauthorised access (fraud), i.e. who is responsible
- how to file complaints

PSD2 focuses on digital payments, e.g. non-cash payments using payment instruments such as cards, credit transfers, direct debits, etc. that can be made in person or via online banking, e.g. via a mobile phone.

Since the adoption of PSD2, the payments market has continued to evolve with new players entering the market, more advanced payments technologies (such as contactless) emerging, and payments needs changing. These market changes warrant an in-depth analysis.

The review aims to assess the effectiveness, efficiency, costs and benefits, coherence and the EU added value of the Directive. It will determine if the PSD2 objectives have been achieved or if changes are needed (and if so, the type and scope of changes). Any forward-looking aspects will also consider the Commission's ongoing work on the open finance framework.

The review will have two dimensions. It will be backward-looking (evaluating the application and impact of the Directive) and forward-looking (assessing the need for possible legislative amendments ensuring that EU retail payment rules remain fit for purpose and future-proof).

As regards open finance, the revised PSD2 opened up access to customers' payment accounts data, enabling third-party information and financial service providers to reuse this data with the customer's agreement. The general purpose of this data reuse was to offer competing financial services or information services, such as comparison tools and data aggregation across several providers. Thus, the PSD2 effectively laid the ground for 'open banking', or the principle of third-party access to customer data in the area of banking products and services. Open finance as a concept is broader and goes beyond the scope of payments account data in the revised PSD2, as it could cover a range of financial services, such as investment in securities, pensions and insurance.

In 2020, the Commission set data-driven finance as one of the priorities in its [digital finance strategy](#) and announced an open finance framework legislative proposal. As reiterated in the [capital markets union \(CMU\) Communication of November 2021](#), the Commission is now accelerating this work as an integral part of the European financial data space. In the broader framework of the [data strategy for Europe](#), the objective is to

make the most of the data economy for EU capital markets, consumers and businesses. Building on the PSD2, this will ensure that more data are available for innovative financial services. It will also give consumers more choice and help them find products that best fit their investment preferences (including sustainable products), while continuing to give them control of their data, including who can access it. This should directly contribute to increasing retail investment.

## CONSULTATION QUESTIONS

### 1. PAYMENT METHODS

Please note that the currency used in this consultation is the euro.

1. How do you usually pay for goods and services? For each payment method, please indicate how often you use it – ‘1’ for the payment method that is your preferred option, and you use most often, ‘2’ for when sometimes use this method, and ‘3’ for never.

a) In a physical shop

1= preferred option; 2= sometimes; 3: never; 4:don't know/no answer.

	1	2	3	4
Cash				
Payment card (debit or credit)				
Digital wallet on mobile phone				
Other payment solutions, please specify [max 100 words]:				

b) Online

*1= preferred option; 2= sometimes; 3: never; 4:don't know/no answer*

	1	2	3	4
Payment card (debit or credit)				
Digital wallet on mobile phone				
Digital wallet on PC or laptop				
Bank transfer				
Other payment solutions, please specify [max 100 words]:				

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	Don't know/no opinion
No	

[should only open if they choose 'no'; open text box; max. 150 words;] Please explain your answer

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

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

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

3.2. What do you think about new companies, including big tech companies, entering the payments market? [open text box; max. 150 words]

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 access 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.

3.3. Do you use AISPs and/or PISPs?

I only use AISP(s)	Yes, I use AISPs and PISPs	I don't know
I only use PISP(s)	No	

[should only open if they choose 'no'] If you do not use AISPs and/or PISPs, what are your reasons for this?? Multiple answers are possible.

I don't need their services	No opinion
I don't trust those providers	Other, please specify [max 100 words, box

	should open if respondent selects 'Other']:
I don't want to share my data with other companies besides my own bank	
I did not know these providers exist	

## 2. DIGITAL PAYMENTS

Do you make digital payments?

Yes	Don't know/no opinion
No	

[if Yes, reveal following questions, if no, please continue to Section 4 on Open Finance]

4. 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.

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.

*1= strongly agree; 2= somewhat agree; 3: neutral; 4: somewhat disagree; 5: strongly disagree; 6: don't know/no opinion/not relevant.*

	1	2	3	4	5	6
Making digital payments has become easier						
It has become easier to make digital payments to other EU countries (e.g. when buying from an online shop in another EU country)						
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)						
It has become easier to transfer money to other EU countries						
It has become easier to transfer money to non-EU countries						

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.

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

*1= strongly agree; 2= somewhat agree; 3: neutral; 4: somewhat disagree; 5: strongly disagree; 6: don't know/no opinion/not relevant.*

	1	2	3	4	5	6
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						

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? [open text box; max. 150 words]

4.2.2. Do you require additional information before making a payment? If yes, please specify [open text box, max. 100 words]

Yes	Don't know/no opinion
No	

[if yes, open text 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.

4.3. What is your opinion about confirming your payment with SCA? [single option selection]

a) When buying something in a physical shop:

It is easy, and I have no problem with it	Other (please specify) [max 100 words]
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	
No opinion	

b) When buying something online:

It is easy, and I have no problem with it	Other (please specify) [max 100 words]
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	
No opinion	

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.

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	Don't know/no opinion
No	

4.3.2. Do you believe payment service providers should put in place more security measures? If yes, please explain your answer and include any

suggestions. [should open if respondent chooses ‘Yes’; open text box; max. 150 words]

**Contactless payments** are payments made without inserting your card into a payment terminal. Some low-value contactless payments (usually below EUR 50) can be exempted from SCA, not requiring your PIN.

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.

4.4. What do you think about the maximum amount for a contactless payment (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. [single option selection]

The EUR 50 limit should remain	The limit should be higher than EUR 50
The limit should be lower than EUR 50	I should be able to set my own limit
	Other (please specify) [max. 100 words]

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.

4.4.1. 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’.

<b>Value in euro</b>	<b>Number of consecutive payments</b>
The limit should be lower than EUR 150	This should be less than five consecutive payments
The limit should be higher than EUR 150	This should be more than five consecutive payments
I should be able to set my own limit (including EUR 0)	I should be able to set my own limit (including zero payments)
Other, please specify [max 100 words]	Other, please specify [max 100 words]

## 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 block a certain amount before you fill up your tank. The blocked amount will then be corrected, and the exact final payment will be processed afterwards.

4.5. Should there be a limit on the amount that can be blocked? [single option selection]

Yes [show text box if selected], and the limit should be:	Don't know/no opinion
No, no limit is needed	Other (please specify) [max 100 words]

## Fraud

4.6. As a consumer, have you been a victim of payment fraud recently? [single option selection]

Yes	Don't know/no opinion
No	

4.6.1. [should only open if a is 'Yes', if 'No' or 'Don't know/no opinion' go to 11] If yes, please give more details [open text box; max 250 words]

4.6.2. If you were victim of a fraud (otherwise go to question 11) [single option selection], did you ask your payment service provider for a refund?

Yes, and I received a full refund	No, I did not request a refund
Yes, but I only received a partial refund	Don't know/no opinion/decline to answer
Yes, but I did not receive any refund	
Yes, but I requested a refund from another party (please specify) [max 100 words]	

4.6.3. Were you satisfied with the refund process (requesting the refund, communication with your payment service provider, length of the process, etc.)? [open text box; max. 150 words].

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

*1= strongly agree; 2= somewhat agree; 3: neutral; 4: somewhat disagree; 5: strongly disagree; 6: don't know/no opinion/not relevant.*

	1	2	3	4	5	6
Making digital payments has become more secure						
My payments data is adequately protected						
Strong customer authentication has helped make digital payments safer and more secure.						
For digital payments, convenience and speed are more important than security.						

4.7.1. Please explain your answers and include any proposals you may have that further protect digital payments. [open text box; max. 250 words]

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):

4.8. Do you have specific concerns about the payments market and recent market developments? e.g. are there (new) risks that require special attention? [open text box; max. 250 words]

4.8.1. What is your opinion about the level of regulation of the payments market? Is it sufficient or is there too much regulation?

### 3. OPEN FINANCE

Open finance refers to a customer allowing their data to be shared or re-used 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-to-business 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 better-targeted 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.

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)? Question 15. 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?

Account/data type	Yes	No	Don't know
Savings account data			
Mortgage loan data			
Consumer credit data			
Securities account data			
Pension data			
Insurance data			

Please explain your answer. [open text box] [max 100 words]

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	Don't know/no opinion
No	

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

Yes	Don't know/no opinion
No	

Please explain your answer. [open text box] [max 100 words]

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	Don't know/no opinion
No	

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

Yes	Don't know/no opinion
No	

9.1.1. If not, how could this best be ensured? [open text box – max 100 words]

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).

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	Don't know/no opinion
No	

Please explain your answer. [open text box] [max 100 words]