Factual summary report PSD2 and open finance public consultation

This document should be regarded solely as a summary of the contributions to the public consultation on a review of PSD2. It cannot in any circumstances be regarded as the official position of the Commission or its services. Responses to the consultation activities cannot be considered as representative sample of the views of the EU population.

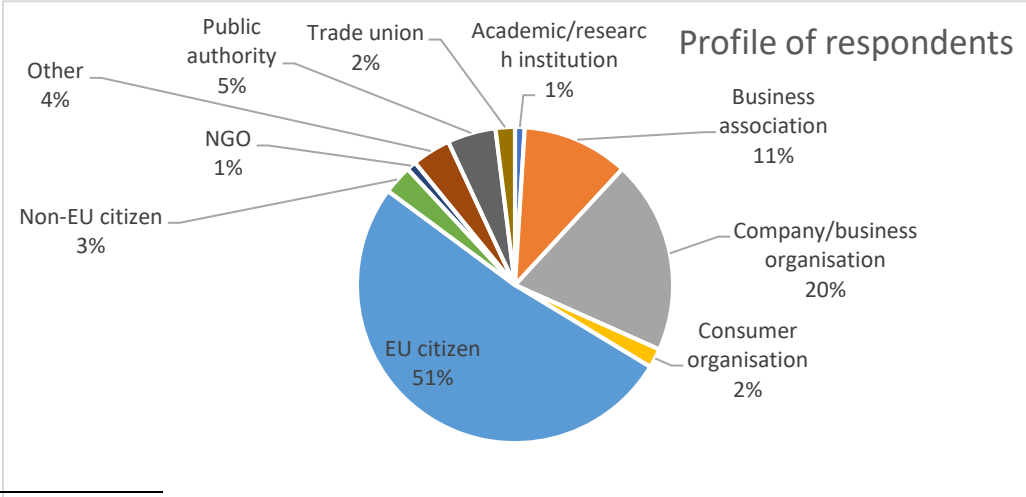
1. Introduction

As part of its work on the review of the Revised Payment Services Directive (hereafter – PSD2) and the Commission's work on open finance, the Commission held a public consultation on the various aspects pertaining to the application and impact of the PSD2 and to inform the work on open finance. The consultation period lasted 12 weeks (10 May 2022 - 2 August 2022).

The aim of Section 1 and Section 2 of the consultation was to gather views from a broad range of stakeholders on whether the PSD2 continues to meet its objectives in terms of competition, innovation and consumer protection, and if it is still fit for purpose and future-proof. The public consultation was also used to collect evidence to assess, in line with the Better Regulation principles, the effectiveness, efficiency, coherence, relevance and EU value-added of the PSD2. The aim of Section 3 of the consultation was to gather views from the general public and interested professional stakeholders on open finance, thereby also complementing the Commission's targeted consultation on open finance.

2. Respondents

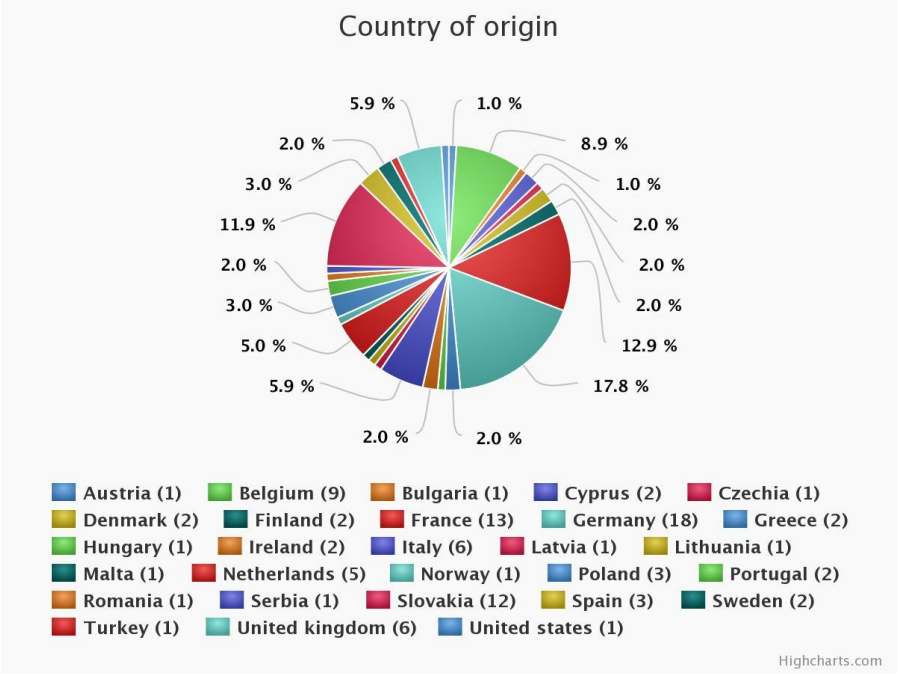
In total, 101 respondents replied to the public consultation. EU citizens (52) formed the largest group of respondents, representing 50% of all respondents. Individual companies (20) and business associations representing their interests (11) formed the second largest group of respondents, representing together 30% of all respondents. There were also 5 public authorities (incl. the Danish Ministry of Industry, Business and Financial Affairs), 2 consumer organisations (both EU-focused), 3 non-EU citizens, 2 trade unions (both EU-focused), 1 academic/research institution, 1 NGO (a charity) and 4 others (2 law-related businesses, a risk management business association and 1 citizen who appeared to have mislabelled itself[1]) who participated in the consultation (see Figure 1)



[1] Labelled "other", with organisation name "Občan EU", which translates to EU citizen in Slovakian.

Responses covered a wide range of business companies, their associations and fields of activity (multiple responses possible). Many respondents are active (amongst others) in a non-defined field (Other – 43, Non-applicable – 20, total 62%), 28 respondents are active in Banking (28%) and 10 in Insurance (11%). Other fields of activity indicated are pension provision (4 replies), accounting (3), investment management (3), auditing (1) and credit agency (1). Among those that labelled their activities as "Other" or "Non-applicable" are for example legal firms/lawyers, software vendors, EU-citizens involved in payments, associations for travel agencies, -vending machines and -telecommunications, and an association and a firm involved in electrical vehicle charging infrastructure.

The vast majority of all responses came from within the EU (92%, 93 replies), covering 25 Member States. 6 responses came from the United Kingdom, 1 from Turkey and one from the United States (although this response was incomplete). Most responses came from Germany (18), France (13) and Slovakia (12). The above-average response rate from Belgium (given the size of the country; 9) can be explained by their activity: all 9 respondents have, in different ways, an EU focus or coverage.



3. Preliminary results observed in the public consultation

The public consultation was divided into 2 topics: PSD2 and Open Finance. The outline of the consultation was as follows.

1. PSD2: Payment Methods
2. PSD2: Digital Payments
    a. Blocking Funds
    b. Fraud
3. Open Finance

Respondents mostly provided feedback to the main topics: payment methods (94 replies), digital payments (92) and Open Finance (92). The subsections on blocking of funds and fraud received fewer responses (66 each). Without prejudice to the more in-depth analysis of the replies that will be carried out in due time, the following are general preliminary results from the public consultation.

3.1. Payment methods

For payment methods in a physical store, the largest group of respondents (38 replies, 40%) indicated that their first preference is to pay by card (debit or credit), digital wallets on a mobile phone come in second (23 replies, 24%), closely followed by cash (21 replies, 22%). For most respondents, cash is the second preferred payment option (35 replies, 37%), whereas a significant proportion of respondents indicated they do not prefer to pay using a digital wallet on their mobile phone (22 replies, 23%). Other payment solutions are not popular or unknown to the respondents: 67 indicated don't know/no opinion/not applicable or provided no answer (71%).

For online payments the preferred method is by payment card (debit or credit) with 49 replies (52%). Zooming in on EU-citizens, this is even higher (38 out of 55 replies, 69%). Bank transfer is the preferred second option (37 replies, 39%) – only 12% (11 replies) indicates this is their number 1 preferred option. A large group of respondents does not like to pay online using digital wallets, either on mobile phone (33 replies, 35%) or on PC or laptop (34%, 32 replies).

Those that indicate to make use of other payment methods for online payments mention (25 replies, 27%), amongst others, buy-now-pay-later (BNPL), peer-to-peer mobile payment apps, cryptocurrency, or a bank transfer via a payment initiation service provider (PISP).

Most respondents find the payment market innovative enough (51% yes – 48 replies, 30% no – 28 replies), and also find that the choice in payment services has increased over the last 5 years (70% yes – 66 replies).

When asked about their attitude towards new companies, including big tech companies, entering the payments market the overall sentiment is positive, but there are concerns about the (non-EU) big tech companies, a.o. on data privacy and big techs could become too powerful.

The questions on PSD2-services providers, Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) received fewer responses (66). The results show that 30 respondents use either or both services (45%), the remaining either don't use the services (24 – 36%) or don't know/don't provide an answer (9 and 3, 14% resp. 5%). The most common reason provided for not using these services is that people do not want to share data with other companies than their own bank (15 responses – 23% out of 66. 14 out of 15 responses are from EU-citizens) and that they don't trust these providers (12, 14%). Elaborating on these explanations two respondents note that the AISP and PISP services often do not work due to poor integration with ASPSP PSD2-interfaces.

3.2. Digital payments

The majority of respondents (92) makes digital payments (67 replies, 73% - 41/67 are EU citizens), against 11 explicit no's (12%, of which 7 EU citizens).

Most of the 67 respondents making digital payments find that making digital payments has become easier (79% - 53 replies, 6% - 4 replies- disagrees). Follow-up questions concerned experience with making cross-border digital payments to other EU countries (69% find it has become easier – 46 replies, 7% disagrees – 5 replies), and to non-EU countries (28% agrees it has become easier, 12% disagrees and 25% is neutral, resp. 19 replies against 8 and 17 replies).

Regarding information and fees, the views lean towards the negative side. When asked whether the cost of fees in general was clear, 35% (23 replies) disagreed, of which 24% (16 replies) strongly disagreed. For payments that involve a currency conversion, the feedback is even more negative: 46% (30 replies) found it unclear what exchange will be applied, against only 14% (9 replies) who do find it clear.

Respondents elaborate on why they find the information provided insufficient, often referring to unclear exchange rates at ATMs or when using a credit card, or that an exchange rate is provided, but the reference rate is not. Others refer to missing merchant information and that there are still hidden fees.

Those that would like more information (39%, 25 replies) would like to know the exact execution time, the exact amount of fees per transaction step, the conditions of the payment (recurring or not, if the price can increase in the future, how to cancel), some kind of confirmation that the website if not fraudulent, the reference exchange rate.

SCA

The public was also asked about their experience with performing SCA, strong customer authentication, during payments (64 respondents).

For physical, in-store payments 44% indicate they find it easy (28 replies), against 30% (19 replies) who find it cumbersome. However, 23% (15 replies) out of that 30% accepts SCA as a fraud preventive measure. 20% indicates "other" (13 replies). The view is almost exactly the same for SCA during online payments (although more respondents find it cumbersome, but worth it given fraud prevention – 22%, 20 replies).

In additional commentary respondents mention that applying SCA for payments is in principle a good measure, but note that SCA depends on network connectivity, and that the way SCA is implemented should be allowed to innovate, e.g. through biometrics, where another notes the application of SCA should be left to the merchant or its PSP (and also take on the liability). A business association notes that a too complex SCA experience could lead to PSUs being "*pushed towards using Big Tech wallets (Apple, Google etc) instead*". One respondent, an association of vending machines, points out that their type of transaction, often low value and very low risk, should also be exempted from SCA, instead of having to invest in new PIN pads/terminals.

Most respondents agree that PSPs should be required to not just offer a mobile phone-SCA solution: 38% (35 replies) against 23% (21 replies). Those that agree refer to the newer fraud methods (e.g. social engineering), where SCA does not protect against, that regulation should support the development of new security measures and that no specific technological solutions should be mandated (also keeping in mind that SCA solutions should cater for all user groups).

Contactless

The views on the maximum limit to contactless payment (currently 50 EUR) are mixed. Many want to set their own limits, both in terms of limit per transaction (currently 50 EUR), for the cumulative limit (currently 150 EUR) and for the number of consecutive payments (currently 5). Overall, the desire for an explicit lowering of the limits is stronger than the desire for higher limits. Those that responded to "other" also often mention that PSUs should be able to set *lower* limits.

Suggestions for change are, a.o., that the regulation should allow for different limits between Member States, as price levels differ, that a higher limit (if set by the PSU) should be accompanied with a shift in liability, and another respondent finds the decision should be left with the bank.

3.2. Blocking of 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. The final exact payment will be processed afterwards. Consumers have complained that this can sometimes take a long time

66 respondents provided feedback to the questions on the blocking of funds. Views on the matter are mixed: 29% (19 replies) finds there should be a limit to the amount of funds that can be blocked, 33% (22 replies) find there should not be a limit (38% indicate "other" or "don't know", 25 replies). From the perspective of EU citizens views are mixed: 37% (15 replies) finds there should not be a limit, against 34% (14 replies) who find there should be a limit.

3.3. Fraud

17% of the respondents (11 out of 66) indicate they have been the victim of fraud recently. Out of those 11, 4 requested a refund with their payment service provider and received this in full. 3 filed a request but did not receive a refund. The others did not file for a refund, where one indicated that they did not know where such a claim should be filed.

The types of fraud respondents suffered differ: some purchased something online, but never received the product or service, others talk about being charged without authorisation.

The overall sentiment about security within payments is positive: most respondents feel that digital payments have become more secure (42 replies, 64%), and that strong customer authentication (SCA) has helped to make digital payments safer and more secure (50 replies, 76%). Respondents are less positive about their payments data being protected (30 replies or 45% agree, against 42% who are neutral or disagree, 28 replies).

3.4. Open Finance

The majority of citizens respondents argued that financial service providers holding data should be obliged to share them with other financial or third-party service providers, if consumers have given their consent or agreement (55%, 30 out of 55 replies). However, citizen respondents are concerned to share financial data due to a lack of trust which stems from concerns over privacy, data protection and digital security, and a generalised sense of not being able to control how their data is used. An overwhelming majority of citizens responding to the public consultation believe there are security and/or privacy risks in giving service providers access to their data (84%, 46 out of 55 replies). Moreover, most citizen respondents do not believe that financial service providers that hold their data always ask for consent before sharing those data with other financial or third-party service providers (57%, 26 out of 46 replies).

To ensure trust in data sharing, citizen respondents suggested a range of solutions strengthen consumer consent/agreement. Solutions typically cited included: (1) The introduction of consent management tools that builds trust, transparency and user ownership of all data concerning them; (2) There should be a high-level system in which all data holders and users are intensely monitored and supervised; (3) There should be a technical mechanism that prevents data from being repurposed; (4) There has to be strict compliance at all times with the GDPR.

Professional respondents were more favourable to data sharing and citied benefits with regards to competition and better customer journey resulting from greater innovation in financial products and services. However, certain professional respondents also voiced concerns over competition from new entrants, security risks and data misuse that could result from greater data sharing in the financial sector.

4. Other

The public consultation was published on the Have Your Say page if the Revised Payment Services Directive and the Have Your Say page of the Open Finance initiative. The consultation was promoted via social media channels such as the European Commission's Linked-In page and Twitter account. These posts could be and were reposted by various members of the commission and other interested parties.

Next to the public consultation there were also two separate targeted consultations (one on PSD2, one on Open Finance). Both initiatives also received two separate responses to a dedicated Call for Advice from the European Banking Authority. The PSD2 review also included an external study. Furthermore, both initiatives gathered information from stakeholders via expert groups and bilaterally.

Having received all input from the market about the PSD2 and Open Finance, both initiatives will review and where possible and feasible incorporate this feedback into their assessments of the PSD2 and the Open Finance framework. This work will be included in a synopsis report.

The factual summary report of the public consultation and the responses provided are published on the Commissions Have Your Say page (PSD2).