The European Consumer Organisation

The Consumer Voice in Europe

CONSUMER-FRIENDLY OPEN BANKING

ACCESS TO CONSUMERS’ FINANCIAL DATA BY THIRD PARTIES

Contact: Jean Allix – Farid Aliyev – financialservices@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d’Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2018-082 - 20/09/2018

Why it matters to consumers

One of the biggest recent technological developments in retail finance is 'open banking', where third party firms (FinTechs and others) access consumers' bank account data and offer various services. These may include payment initiation, money management and investment advice, credit and insurance products, or cheaper energy offers. This development has happened through the revised Payment Services Directive (PSD2) which requires banks to grant third parties access to bank accounts based on the consumer's consent, with the aim of promoting market competition. These new developments present both opportunities and challenges for consumers, and should, therefore, be regulated properly.

Summary

This paper sets out BEUC's requirements for a consumer-friendly open banking environment, in which consumers would be in full control of their bank/payment account data. BEUC recommendations are as follows:

- Open banking in the EU should use only the redirection authentication method. This means the consumer connects directly to his home banking, and the consumer's personalised security credentials are not shared with any third party.
- The consumer's consent should be explicit and specifically state which financial data the consumer has given the third party access to.
- The Application Programming Interface standard – a communication channel between the consumer's bank and third parties - should enable third party service providers to provide the consumer's bank with the terms of the consumer's consent.
- The API standard should allow consumers to instruct their bank to refuse access to a particular service, being another bank or a third party service provider.
- The consumer's bank should maintain a list of all service providers who have access to the consumer's financial data.
- The consumer should be able to cancel at any time any specific agreement given to a third party. The API standard should require that, when an agreement is cancelled by the consumer, the party which has received the cancellation (the consumer's bank or the third party) should inform the other party.

The Consumer journey reflecting BEUC's recommendations would look as follows:

1) The consumer enters into a contractual relationship with the third party and gives his/her explicit consent for the third party to directly access his/her payment data.
2) The third party sends a request to the consumer's bank to directly access the consumer's data.
3) The consumer logs in to his/her online banking facility and is presented with the request from the third party to access his/her data (redirection) and the agreement he/she has given.
4) The consumer activates the request by specifying exactly (ticking boxes) what data the third party is allowed to access (cluster).
5) The TPP can now freely access the authorised consumer data.
6) At any time, the consumer can log in to his/her online banking facility and untick boxes or completely block the third party from access.

TERMINOLOGY

Term	Definition
AIS	Account Information Service
API	Application Programming Interface. The basis of the digital economy to establish connections between applications.
API EG	The API Evaluation Group set up by the European Commission. All the final documents of the API EG are available online.
ASPSP	Account Servicing Payment Service Provider. It means a bank in common language.
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. This shall be done by using the strong customer authentication rules (2 out of the 3 factors, i.e. what I have, what I know and what I am).
EBA	European Banking Authority
GDPR	General Data Protection Directive
PIS	Payment Initiation Service
PSD2	Revised Payment Services Directive
PSU	Payment Service User
RTS on SCA and CSC	Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication
SCA	Strong Customer Authentication
Screen scraping	The access to the data by using the User Interface
User Interface	The home banking channel used by the consumer to access his bank account
TPP	Third Party Provider

1. What is open banking?

The revised Directive on Payment Services[1] (PSD2) enables Payment Initiation Services (PIS) and Account Information Services (AIS) to access consumers' online banking data to be able to provide their services requested by the consumer. It also states that these two types of services (hereafter described as TPP services) can be provided by banks themselves.

A PIS allows consumers to pay by credit transfer when shopping on a merchant's website if the merchant offers this method of payment. The best known PIS are iDEAL (in the Netherlands)[2] or Sofort (in Germany).[3] The former is an interbank system, the latter an independent system. The essential feature of a PIS is to use the credit transfer payment instrument, which is much cheaper for the merchant than a card payment.

An AIS aggregates information from the consumer bank's account(s) for performing the service requested by the consumer. It can be advice on money management, credit scoring, access to targeted credit offers, insurance comparison, etc.

Before PSD2 and even today when consumers agree to give access to their account, PIS and AIS are using the home banking channel (which consumers use when connecting to their online banking). They will have access to the same information as that available to the consumer when using his/her home banking (this is called screen scraping). As many banks refused to give this access to third parties, the activity of PIS and AIS was limited before PSD2. The great innovation of PSD2 is to require banks to grant that access to a PIS or an AIS to open competition. This is now a consumer right. PIS and AIS are now regulated under PSD2 which sets provisions related to their obligations and liabilities in case of incidents.

PSD2 mandates the creation of a new channel for communication between the consumer's bank and the AIS and PIS. The legislation[4] refers to a "dedicated interface". In the banking world this channel is called API (Application Programming Interface). As the United Kingdom is ahead in implementing its own Open Banking project[5], the term 'open banking' is also used. This expression corresponds to a new reality, where the bank becomes open to third party providers (FinTechs). The idea of open banking is not limited to Europe, it is also being explored in several other countries outside Europe.[6]

2. Background of the debate

Prior to PSD2, the only channel available for PIS and AIS to access the consumer data was home banking. BEUC, while agreeing that PIS provide a useful service to the consumer, has always opposed that the access is done through the consumer's home banking. There are two reasons for this. First, the consumer's confidential data for identification (security credentials) is passed to the PIS. Secondly, because of screen scraping, the PIS could read all the information available on the consumer's home banking (current account transactions, savings account, running credit contracts, insurance contracts, etc.).

[1] Directive 2015/2366 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN
[2] https://www.ideal.nl/en/
[3] https://www.klarna.com/sofort/
[4] RTS – Regulatory Technical Standard, level 2 implementing measure setting the details of the PSD2 provisions.
[5] https://www.openbanking.org.uk/
[6] See a map on page 15 of this study by Innopay and Deutsche bank: http://www.cib.db.com/insights-and-initiatives/white-papers/unlocking-opportunities-in-the-api-economy.htm

For these reasons, last year when the discussion on the communication channels between banks and TPPs began, BEUC proposed that the communication be done by a channel (dedicated interface) which should be identical for all banks.[7] Otherwise, each PIS or AIS would have to adapt their system to the specific channel of each bank, which would be technically impossible. At that time many stakeholders were reluctant to accept this idea for a single solution. Nowadays there is a consensus on this idea initially proposed by BEUC.

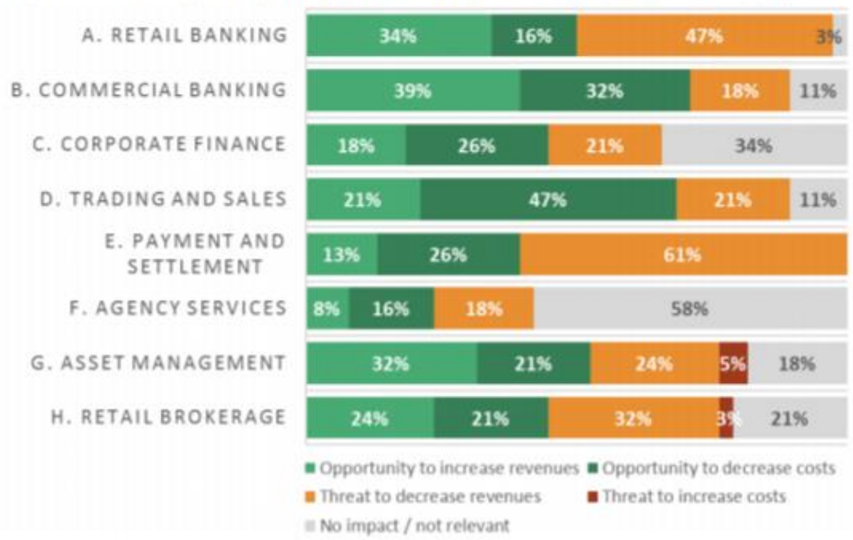
The PSD2 required the EBA (the European Banking Authority) to define the general principles of this new channel. After very long discussions a new regulation was published on 13 March 2018 to come into effect on 14 September 2019.[8]

Defining the technical modalities for the implementation of this open banking was crucial. As a first step, a working group on PIS only was set up under the auspices of the ERPB in December 2016.[9] This group, where the banks and the PIS and AIS were in broad disagreement, eventually came to the conclusion that it is by comparing the different national open banking projects that a solution could be found. This led to the creation of a new working group (API EG - API Evaluation Group) under the auspices of the European Commission.[10]

BEUC participates in this working group aiming to develop a standardised European API (Application Programming Interface). The mandate of the group is: "*… to evaluate standard APIs in order to help ensure that they are compliant with the requirements of the revised Payment Services Directive (PSD2) and meet the needs of all market participants". As a* result, the group will: *"make recommendations aimed at API specifications convergence on a European level and to help establish harmonized market practices."* For BEUC, the important point is "*the need of all market participants".*

The debate between incumbent banks and TPPs (FinTechs) is intense. The following graph shows the banking sector is strongly concerned by competition coming from TPPs in the field of retail payments.

Figure 2. *How do you see FinTech firms affecting the current business model (business lines) of your bank?*



Source: EBA report on the impact of FinTechs on incumbent banks business models, July 2018.

[7] BEUC letter to Commissioner Dombrovskis, May 2017: http://www.beuc.eu/publications/beuc-x-2017-054_mgo_psd2_-_secure_communication_between_banks_and_third_party_psps.pdf

[8] Commission Delegated Regulation EU 2018/389 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

[9] Euro Retail Payments Board, of which BEUC is a member: https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html

[10] https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-03/API%20EG%20002-18%20v1.2%20Terms%20of%20Reference%20API%20Evaluation%20Group_0.pdf

3. Open banking and consumer interest

Open banking is a new concept in the field of financial services. The first question to ask is what are the advantages for consumers?

BEUC always supported services such as payment initiation services (PIS) which bring more competition to the market. That said, we drew attention to the issue of security of consumer's personal credentials. This must also be seen in the light of the fact that consumers are less protected when using credit transfers compared to direct debit and card payments. In the past few years, many consumers have been tricked into transferring money to fraudulent accounts. No redress is provided to consumers in that case.[11]

As regards AIS, they could have potential benefits for consumers, but there are also controversial aspects. An AIS can analyse the consumer's banking data and based on that analysis provide money advice or offer credit or insurance products to the consumer. The consumer interest can be that AIS might increase competition for consumer credit and deposits/savings, through allowing providers access to consumer bank account data. For example, in the case of credit, access to bank account data will allow alternative providers to get much better information of consumer credit risk than is currently available.

But the AIS is also accessing sensitive information, contained in consumers' bank accounts, such as information on health conditions, political affiliations, and personal relationships.

An important point is that any bank can act as a PIS or an AIS. If a retailer decides to work with a bank as a PIS, he will be paid by credit transfer, a solution which is much cheaper than classic card payments. If a bank decides to act as an AIS, it will allow the consumer to access all his accounts by using only the mobile app of this bank. The drawback is that this bank will have access to the consumer's data in other banks.

4. The authentication

The mechanism provided by open banking is approximately as follows:

- The consumer gives his consent to the TPP indicating his/her bank's name. The TPP, using the open banking channel (API), connects with the bank. The bank will not receive the consumer's consent and cannot ask for more information. It is a contractual relationship between the TPP and the consumer, the bank can only provide the requested information, once the authentication is successful.

- The next step is the authentication of the consumer, using the bank credentials. There are 3 solutions available:
  - Redirection. This means the consumer is connected directly to his/her bank, through home banking (like with iDEAL).
  - Decoupled. This means the consumer is connected directly to his/her bank through home banking, but the authentication is done through another device (phone). This is the case, for example, where the authentication is done via smartphone using biometrics (fingerprint, iris, etc.).
  - Embedded. The consumer's personalised credentials are sent to the bank through the TPP. The embedded approach introduces additional security risks,

[11] See for example Which? super-complaint submitted to the UK regulator, 2016: https://www.psr.org.uk/sites/default/files/media/PDF/which-super-complaint-sep-2016.pdf

as in that case a third party is handling, storing and transmitting the consumer's personal security credentials.

For consumers the key question is security and whether any third party can get access to consumers' personalised security credentials. The PSD2 states that the TPP must ensure those credentials are not accessible to parties other than the user and the issuer and that the TPP will transmit it through safe and efficient channels.[12] Nevertheless, we consider this is too risky.

For BEUC, the only really secure solution is redirection (and, where warranted, the decoupled method as a variant of redirection), in other words, where no personal credentials are shared with any TPPs. But the API will have the obligation to support the 3 methods. It will then be up to the banks to choose which one they will implement.[13]

BEUC recommendation #1:	The EU open banking should use only the redirection authentication method.

5. The consumer's consent

For the time being, the main issue related to open banking is the consent of the consumer. Are we sure that the consumer knows exactly what he/she is giving his agreement to?

A very recent study on open banking by BEUC's UK member the Financial Services Consumer Panel shows that this is not at all the case. The research showed that consumers are not giving informed consent when they share their financial data. Most people did not read terms and conditions and did not understand them even when they did. They saw terms and conditions as too long and complicated, full of legal jargon, and 'not written with consumers in mind'.[14]

Another recent study, by BEUC's German member vzbv, came to similar conclusions. The survey was assessing what consumers think they are consenting to with e-payment providers based on the knowledge of the terms and conditions.[15]

PSD2 indicates that the consent of the consumer has to be explicit. There is no definition of 'explicit' in this case. Our recommendation 2 below is a way to translate in practical terms the word 'explicit'. The other conditions for consent provided by the GDPR have, of course, to be met.

The Article 29 Working Party[16] adopted on 10 April 2018 the final version of the guidelines on consent under GDPR.[17] On page 19, there is a very good example (n°17) of an explicit

[12] Article 66.3.b and 67.2.b of PSD2

[13] Report of the API EG on the strong customer authentication: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-05/API%20EG%2030-18%20Authentication%20guidance%20%28SCA%29.pdf

[14] FSCP position paper and recommendations, April 2018: https://www.fs-cp.org.uk/press-release-consenting-adults-consumers-sharing-their-financial-data

[15] https://ssl.marktwaechter.de/digitalewelt/marktbeobachtung/e-paymentwie-sicher-sind-unsere-daten-beimbezahlen-im-netz

[16] The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC (Data Protection Directive). It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

[17] Guidelines on Consent under Regulation 2016/679: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

consent given by the consumer in front of a screen. Our proposal copies what is proposed by this example.

The informed consent is the most important dimension of the trust in open banking. A tick in a box saying that the consumer accepts terms and conditions of a document he will never read is not at all an informed, explicit and specific consent.

BEUC recommendation #2	The consumer's consent should be explicit: 'by ticking this box, I agree that company "XXX" will have access to the following financial data *(list data for which the access is being requested)* managed by the ASPSPs (bank) "YYY"

Another important aspect is to make a distinction between authentication and the consumer consent. The authentication does not mean the consumer has consented. The authentication does not allow the consumer's bank to know exactly what the consumer has given his agreement to. The consumer consent has to be handled completely independently of the authentication.[18]

In the current situation the bank does not know exactly what the consumer has given his consent to. Is it access by the TPP to the account balance or to all the payments transactions? Access to past payments or also payments scheduled?

The counter argument is that the authentication means consent. This argument can be valid for the payment initiation service as it is a one-time transaction and it is an agreement on an amount to be paid. In case of a payment, the TPP needs to know if the funds are available on the consumers' account. With the growing use of instant credit transfer, the PIS will know immediately if the payment has been executed. Thus, the PIS will not need to check the availability of funds on the consumer's account anymore. It does not need to know the account balance, for example.

As for AIS, the access to data should be limited to data necessary to perform the service requested by the consumer. For example, a third party savings account provider or intermediary would not need access to all payment transactions on the consumer's payment account. It would need to know only the amount and the current interest rate of the consumer's savings account.

BEUC recommendation #3	The API standard should enable the TPP to provide the ASPSP (the consumer's bank) with the terms of consent of the consumer.

There is a risk that some consumers have not understood what they have agreed to. Some consumers may want to be sure that they will never give a right to third parties to access their bank account. To allow that, consumers should have the right to instruct their bank not to accept the sharing of their data with third parties. The same kind of provision exists for direct debit (see SEPA Regulation). Why not for data sharing? There is nothing in the PSD2 or the RTS that prevents that kind of choice by the consumer.

A possible technical issue here might occur if the consumer had asked the bank to block access to his/her account, but nevertheless he/she accepts a proposal by a TPP. In that case, the bank should inform the consumer why it has denied the transaction, so the consumer can withdraw his/her opposition.

[18] In the API Evaluation Group, BEUC has made several proposals regarding the consumer's consent. The documents related to the API EG are available at the following link: https://www.europeanpaymentscouncil.eu/search?qry=&kb%5B0%5D=ctype%3Akb_document&kb%5B1%5D=tags%3A4511

BEUC recommendation #4	The API standard should allow consumers to instruct their ASPSP (bank) to refuse any kind of access, being another ASPSP, an AIS or a PIS.

Additionally, the consumer needs to know to whom he has given access to his financial data. This information provided in a table (or dashboard in the UK open banking) should be provided by each bank.

BEUC recommendation #5	The ASPSP (the consumer's bank) should maintain a list of AIS or other ASPSPs to which the consumer has given access to his bank account. The request sent through the API should include this automatic registration.

Finally, consumers should be able at any time to cancel the agreement they have given, using the table/dashboard of the valid agreements. The other party (TPP, ASPSP) should be informed immediately of this cancellation.

BEUC recommendation #6	The consumer should be able to cancel any specific agreement given to a third party at any time. The API standard should require that when an agreement is cancelled by the consumer to the ASPSP (his/her bank) or the TPP, the party which has received the cancellation should inform the other party.

6. GDPR versus PSD2

6.1. About consent

There is currently a discrepancy over how 'consent' is interpreted in GDPR versus PSD2. PSD2 makes several references to "consent" and sometimes to "explicit consent". Many people seem to consider that the two terms mean the same thing. These two concepts are not identical. In PSD2, Article 64 is dedicated to consent and withdrawal of consent in chapter 2 titled "Authorisation of payment transaction". According to article 66 on PIS, payers (consumer) have to give their explicit consent. According to article 67, AIS provide services only based on the payment service user's explicit consent.

Article 7 and recital 32 GDPR provide details about the requirements for valid consent but do not mention explicit consent. Article 9 provides a list of particularly sensitive personal data of which the processing is prohibited.[19] This article has a list of exemptions. One exemption is if "*the data subject has given explicit consent to the processing of those personal data.*"

Explicit consent is also mentioned in GDPR article 22c as regards profiling. The consumer has the right not to be subject to a decision based only on profiling except if he/she has

[19] GDPR Article 9 provides a list of particularly sensitive personal data of which the processing is prohibited: *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

given an explicit consent. Many consumer credit demands are accepted only on the basis of profiling, using automated tools.

When accessing the consumer’s bank account, the TPP can have access to many data elements related to the beneficiaries of various payment transactions. For example, if a consumer makes regular payments to a political party or has subscribed to a religious magazine, that data might be considered as sensitive under article 9. Another example, healthcare expenses or regular credit transfers to e.g. an association of anonymous alcoholics could also be considered sensitive health data.

This is why BEUC considers that the rule of explicit consent as defined by the GDPR applies to open banking. This means that for consent to be valid it has to meet the following requirements: freely given (consumers should not be forced to give consent to access banking data beyond what it is necessary for the provision of the service); informed; specific; unambiguous (explicit).[20]

6.2. About the scope of the API

PSD2 covers only payment accounts (current accounts) and not "other accounts" such as savings accounts. Consequently, the scope of the work of the API EG is limited to payment accounts. Nevertheless, it is possible for the API EG to extend the scope of its work to other accounts. This is what AISs are requesting. The position of AISs is quite clear: if they cannot use the API for “other accounts” they will use the consumer home banking channel, the old screen-scraping.

In such a situation the only applicable legal text is the GDPR, and not PSD2. As a consequence, work should be done by regulators to ensure that consumers are adequately protected against data breaches, misuse of data, privacy and security risks associated with sharing of consumers’ financial data.

BEUC is in favour of the extension of open banking to data which are not covered by PSD2 such as savings accounts. However, this extension must be done in full transparency and in conformity with the principles we have outlined for the implementation of PSD2.

END

[20] Guidelines on Consent under Regulation 2016/679: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

BEUC The European Consumer Organisation

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).