



The Consumer Voice in Europe

A NEW DIGITAL FINANCE STRATEGY FOR EUROPE / FINTECH ACTION PLAN

BEUC response to the Commission's consultation



Contact: financialservices@beuc.eu

BUREAU EUROPEEN 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-2020-070

Why it matters to consumers

The increased use of data and technology is changing the way that financial markets work for firms and consumers. New developments related to Open Banking and Open Finance have the potential to transform financial markets, with new players entering the market and new services and products being offered to consumers. Digital transformations have the potential to increase competition between firms to the benefit of consumers. However, new risks could emerge related to digitalisation, including data protection and privacy concerns. Safeguards and rights are needed to ensure consumers can benefit from new digital financial services.

Summary

In April 2020, the European Commission published a public consultation on a new Digital Finance Strategy for Europe and FinTech Action Plan. BEUC welcomes the opportunity to comment on the European Commission's new Digital Finance Strategy. Digital innovations mean that financial markets are changing for consumers. New developments related to Open Banking and Open Finance have the potential to transform financial markets, giving consumers new opportunities to compare, switch or use new tools to manage their finances.

The Payment Services Directive 2 (PSD2) first introduced Open Banking principles enabling consumers to consent to third parties accessing their payment account information and established clear technical rules for accessing this consumer data. However, the scope of PSD2 is currently limited to payment accounts. BEUC believes that extending Open Banking principles to other products, such as savings accounts, pension products, insurance products, mortgages and consumer credit help consumers rely on new financial services tools and to more easily compare and switch between financial services providers.

BEUC believes that the European Commission should extend the scope of PSD2 to other financial services products and introduce an Open Finance regulatory regime to ensure that consumers are protected when using new digital financial services. However, wider access to consumer data by third parties must take place in a safe and ethical environment, with the informed and explicit consent of the consumer. To ensure that Open Finance is developed in a consumer-friendly way, clear rights and protections are needed for consumers to ensure that they remain in full control of their personal data. Consumers must be easily able to withdraw consent for data to be shared, and clear liability rules should be established in case of security breaches and data misuse.

Question 1. What are the main obstacles to fully reap the opportunities of innovative technologies in the European financial sector (please mention no more than 4)?

One of the main obstacles preventing the emergence of technology-enabled financial services is access to financial data. PSD2 first introduced a legal environment enabling consumers to consent to third parties accessing their payment account information or making payments on their behalf and established clear technical rules for third parties accessing this consumer data. However, the scope of PSD2 is limited to payment accounts, and does not cover other financial information. BEUC believes that the European Commission should propose specific legislation on the access and use of financial data (open finance) allowing access to all types of financial information, including for savings accounts, mortgage, life insurance, retail investments, pension products, consumer credit, etc. However, wider access to consumer financial data by third parties must take place in safe and ethical environment and under full control of the consumer (with the informed and explicit consent and easy withdrawal of consent, clear liability rules in case of security breaches and data misuse). Clear protections are needed to ensure data protection and privacy of users. For more information on what safeguards are necessary, please read our full response to the consultation.

BEUC members have already identified concerns with regards to the online privacy practices of new digital banks. For instance, our Dutch member, the Consumentenbond, found that new digital banks score much worse when compared to traditional banks when it comes to data protection and privacy. New digital banks often share personal information, such as the consumer's email address and phone number with third parties, such as social media companies and marketing companies. Privacy and data protection concerns could prevent consumers from engaging with new digital companies and must be adequately safeguarded.

Question 2. What are the key advantages and challenges consumers are facing with the increasing digitalisation of the financial sector (please mention no more than 4)?

The digitalisation of the financial sector has the potential to transform the way financial markets work for consumers. The increased digitalisation of the financial sector could help to improve competition among financial services providers. New digital players in financial services could spur innovation, improve competition with traditional financial services providers, and lead to the development of new services for consumers. For instance, the increased digitalisation of the financial sector could facilitate the emergence of objective and independent comparison tools, could assist consumers in identifying products with lower costs, and could improve competition between financial and payment services providers. New financial products and tools could emerge to assist consumers when making financial decisions.

While innovation-based competition in the financial industry can bring new benefits to consumers, there are equally new risks that could emerge for consumers. The financial industry is data-intensive, and the rise of the internet, e-commerce and widespread use of digital technology by consumers and across all business sectors in general has led to an exponential increase in consumer data. BEUC is concerned that digitalisation could go hand in hand with increased use of sensitive data (for instance, in credit score assessment or in insurance) without valid informed consent from the consumer. While the GDPR has strengthened the rules for consent, problems remain in this area and there are gaps in the enforcement of the GDPR rules. BEUC furthermore sees concerns resulting from inappropriate use of artificial intelligence tools. In addition, new cybersecurity or operational risks related to digital services could emerge for consumers and need to be adequately regulated. Another concern is related to confusing/unmanageable online distribution chains making it difficult for the consumer to know how and where to file a complaint, i.e. when it is not clear who is responsible if something goes wrong. This latter point is also linked to inappropriate distribution of the responsibilities between home and host supervisory and dispute resolution bodies in Europe (see our response to other questions).

Question 3. Do you agree with the choice of the below priority areas?

Building on previous policy and legislative work, and taking into account the contribution digital finance can make to deal with the COVID-19 emergency and its consequences, the Commission services are considering four key priority areas for policy action to spur the development of digital finance:

- a) ensuring that the EU financial services regulatory framework is technology-neutral and innovation friendly;
- b) reaping the opportunities offered by the EU-wide Single Market for digital financial services for consumers and firms;
- c) promoting a data-driven financial sector for the benefit of EU consumers and firms; and
- d) enhancing the operational resilience of the financial sector.

BEUC agrees with the priorities identified by the European Commission. However, promoting a data-driven financial sector must be done in a way that ensures consumers remain in control of their data (see question 26 for our concrete proposals). Achieving an innovation-friendly financial services regulatory framework should not be done at the expense of consumer protection. Equally, the European Commission must also ensure enhanced operational resilience of the financial sector, including reliability of digital services for consumers and enhanced cyber-security.

Question 4: Do you consider the existing EU financial services regulatory framework to be technology neutral and innovation friendly?

There is need to update existing rules such as the digital marketing of financial services directive (DMFSD) adopted in 2002 and which is largely outdated. Last year the European Commission conducted an evaluation of the DMFSD. In our response to the EC consultation BEUC proposed to review the DMFSD with the objective to:

- Transform DMFSD into a horizontal legislation harmonising (minimum harmonisation) certain consumer protection rules across financial products, irrespective of their marketing and sales channels, which would complement the sector specific EU laws (PSD2, MCD, CCD, PAD, MiFID, PRIIPs, IDD, PEPP and others);
- Take into account recent technological developments in the financial sector and safeguard financial services consumers from risks related to digitalisation.

The EU anti-money laundering legislation AMLD also needs to be reviewed. For many years BEUC has been calling on the EU policymakers to review this directive to fully harmonise its 'know-your-customer' provisions. This is a necessary pre-condition to facilitate digital on-boarding and distribution of financial services (see response to Q 16).

Question 5. Do you consider that the current level of consumer protection for the retail financial products and services established by the EU regulatory framework is technology neutral and should be also applied to innovative ones using new technologies, although adapted to the features of these products and to the distribution models?

All provisions for consumer protection should be applicable irrespective of the way that financial services are provided to consumers. While certain requirements may need to be adapted in a digital environment, the key goal should be ensuring equal levels of consumer protection when financial services are provided either digitally or through traditional channels. There should be no differences in the level of protections that consumers are entitled to, whether services are provided on an offline or an online basis.

The same reasoning applies to different digital services. Most consumers have no idea which technology is behind the service they are using. Digital or crypto is not the concern of the consumer. It is the regulator's duty to ensure that the service expected by the consumer is provided. Consumers should have the same rights and protection whatever the technology used.

Question 8. In which financial services do you expect technology companies which have their main business outside the financial sector (individually or collectively) to gain significant market share in the EU in the five upcoming years?

Open banking/finance. The so-called account information service providers (AIS) which is a broad category covering various services from account aggregation to product comparison and financial intermediation to provision of financial services to consumers by third parties which are not the consumer's bank. Technology companies are becoming increasingly interested in becoming part of the EU's open finance ecosystem, and BEUC expects more and more technology companies will get an AIS license in the near future to offer payment and financial services based on the analysis of consumers' personal financial data.

Question 8.1 Please explain your answer to question 8 and, if necessary, describe how you expect technology companies to enter and advance in the various financial services markets in the EU Member States:

All GAFAs are now active in the field of payment services. Based on PSD2, they got a licence as a Payment Service Provider, in particular as an Account information Service. AIS is not in itself a payment service but gives access to the consumer's payment data. AIS data is for them the currency of the digital economy - they are investing in payments to get access to consumer financial data.

Question 9. Do you see specific financial services areas where the principle of "same activity creating the same risks should be regulated in the same way" is not respected?

Yes, BEUC is concerned that crypto-assets products are regulated differently compared to other investment products on the market. Investment tokens are a form of asset, share or security with a profit right attached to it, meaning that the owner will receive dividends. The most known are Initial Coin Offerings (ICOs). A bespoke EU regime is needed for crypto-assets that are currently not covered by EU financial services legislation. Where crypto-assets do not currently qualify as financial instruments under MiFID II, consumers could be exposed to significant financial risks, due to an absence of applicable financial rules (such as key investor protections offered under MiFID II). Without an EU framework, there is a risk of divergent national approaches to crypto-asset regulation.¹

In addition, BEUC is concerned that P2P crowdfunding platforms are not regulated in the same way as other crowdfunding platforms in the EU. The European Commission's legislative proposal on crowdfunding only applies to lending or equity-based platforms lending to business, while lending to consumers through crowdfunding platforms is excluded from the scope of this proposal. Reward- and donation-based crowdfunding also fall outside the scope of the current directive. In recent years, the consumer credit market has changed significantly, with the proliferation of crowdfunding platforms offering loans to consumers online. For example, as reported by our French member UFC-Que Choisir, in France high-cost consumer loans between €200-600 are being marketed by peer-to-peer lending platforms, bypassing national legislation. These companies have questionable marketing practices, do not properly assess the borrowers' creditworthiness, and do not include an Annual Percentage Rate of Charge in their loan offers.

Current EU legislation, such as the Consumer Credit Directive, was designed for more traditional forms of lending and may not adequately cover the new risks associated with new forms of online lending. The European Commission has set out in its Consumer Financial Services Action Plan 2017 that it will address concerns associated with lending to consumers through crowdfunding platforms during the forthcoming evaluation of the Consumer Credit Directive. Easy access to online credit for consumers without proper creditworthiness check could pose risks in terms of irresponsible lending resulting in over-indebtedness. BEUC believes that lending to consumers through crowdfunding platforms deserves regulatory attention and should be adequately addressed under the review of the Consumer Credit Directive.

¹ Please read out full position paper on crypto-assets, 13 May 2020:
http://www.beuc.eu/publications/beuc-x-2020-037_crypto_asset_position_paper.pdf

Question 13. Building on your experience, what are the main challenges authorities are facing while supervising innovative/digital players in finance and how should they be addressed?

In a digitalised world and following recent legislative reforms (such as PSD2), sectoral frontiers become increasingly blurred. Thus, tech giants offer financial services and are among the actors of the open banking ecosystem, insurance products are offered as part of energy packages, and the provisions of the data protection legislation (GDPR) impact the practices of all market actors. Against this background, cross-sectoral cooperation among EU and national regulators and supervisors (financial, data protection, horizontal consumer protection, energy sector supervisors) becomes increasingly important. A formal cooperation framework should be set up for that purpose. For example, the ESAs have recently been mandated to cooperate with the European Data Protection Board to avoid duplication, inconsistencies and legal uncertainty in the sphere of data protection (Art 9 of revised ESAs Regulations). New digital technologies bring added complexity for financial services regulators. The technologies deployed and market practices used by digital financial services firms can evolve quite quickly, and this adds increased difficulties from an enforcement perspective (with regulation or regulators always running one step behind). It is necessary to ensure that the EU financial supervisors have sufficient resources and technical expertise as it related to digital finance and need to ensure that they can intervene quickly and effectively enforce the rules.

Besides that, close international cooperation among regulators and supervisors is more relevant than ever. Dangerous and speculative products (e.g. payday loans, crypto-assets, speculative investment products) can reach consumers very easily through social media platforms and other online channels. Since the internet has no borders, foreign providers, including the non-European ones, can easily target EU consumers. This presents a challenge for regulators and supervisors at global level and calls for international cooperation in order to reduce the opportunities for regulatory arbitrage and forum shopping.

See also our response to Q22.

Question 14. According to you, which initiatives could be put in place at EU level to enhance this multi-disciplinary cooperation between authorities?

BEUC advocates for the adoption of a 'twin peaks' model for financial supervision, i.e. the creation of separate EU supervisors responsible for conduct of business and prudential supervision, respectively. See a 2017 [joint letter](#) on the ESAs review co-signed by BEUC and several other consumer and financial user representatives. An alternative option could be to enhance the powers and activities of the Joint Committee of the ESAs. See also our response to the previous question.

In addition, as the digitalisation of the financial sector continues, there will be a requirement for much more multi-disciplinary cooperation between financial supervisors, data protection authorities and competition authorities. Strong co-operation between sectoral authorities and data protection authorities is crucial for effective and meaningful protection of consumers. Such cooperation could take multiplate forms, including for instance, cross-sectoral secondment of officials between data protection authorities and financial supervisors. Especially in the area of insurances, with the rise of Big Data Analysis and artificial intelligence, insurance supervisors will need to work closely with data

protection authorities to ensure adequate enforcement of data protection and privacy rules when selling insurance contracts. Equally, in the area of Open Finance, closer cooperation between ESMA and EBA with data protection authorities will be critical.

Question 15. According to you, and in addition to the issues addressed in questions 16 to 25 below, do you see other obstacles to a Single Market for digital financial services and how should they be addressed?

Most European retail legislation on payments, banking, insurances, investments and pensions emanate from the EU level. Many directives are based on a minimum or targeted harmonisation, allowing Member States to adopt stricter rules justified by the need to better protect consumers. For example, the scope of the 2008 Consumer Credit Directive covers loans between €200-75,000, but Member States had the option to also regulate loans below €200. Many countries used that option in order to curb the short-term, high-cost credit market which targets vulnerable consumers.

However, such national legal divergences are sometimes seen as an obstacle that prevent firms from expanding their products and services across borders.

BEUC is in favour of the (Digital) Single Market, which should however not be to the detriment of consumer protection rules in place. We have often advocated for minimum harmonisation EU laws so that Member States can maintain their strong consumer protection laws in place, or adopt rules that go beyond the EU rules, where needed.

Question 16: What should be done at EU level to facilitate interoperable cross-border solutions for digital on-boarding?

Firstly, the European Commission should replace the EU's Anti-Money Laundering Directives into a single Regulation, with no possibility to derogate at the national level. As these five Directives have allowed each Member States to insert its own additional rules, ('Gold plating'), these national rules have become the first major obstacle for the opening of a cross-border payment account by consumers. BEUC welcomes the European Commission's commitment in its Action Plan on Money Laundering (published 7 May 2020) that it will propose legislation to put an end to fragmentation.

The second obstacle preventing digital onboarding is the lack of digital identity mechanisms which can be used at the national level, but also at the cross-border level. Mechanisms allowing cooperation between public registers and the private sector are needed to set up identification mechanisms. PSD2 made Strong Customer Authentication (SCA) mandatory in order to prevent fraud in electronic payments. In some EU countries, through cooperation between the authority and the private sector, systems have been created, such as BankID in the Nordic countries. In some other countries, banks can use a public registration system to identify the consumer, for example, "Itsme" in Belgium.

Based on the Regulatory Technical Standard of PSD2 (Article 34 of Regulation 2018/389) and the eIDAS regulation, there is the possibility to create a European digital identity service. The use of this service in the financial sector could work by using the channel of communication that banks have set up, i.e. the API (see answer to question 23). It should also help to increase the security of the banking operation, for example in the case of the Strong Customer Authentication made mandatory by PSD2.

Question 20. In your opinion (and where applicable, based on your experience), what is the main benefit of a supervisor implementing (a) an innovation hub or (b) a regulatory sandbox as defined above?

The supervisors get experience on how the technology can be used - for good or for bad. Thus, their guidance becomes more relevant. Innovation hubs and regulatory sandboxes can also assist FinTechs with the launch of their services. However, sandboxes and innovation hubs should never be left alone and/or prevent regulation, and there should always be an arm's length principle: the supervisors should never become part of the business operation.

Additionally, BEUC has concerns that while individual Member States allow some of their FinTechs to play in small sandboxes, the BigTechs are roaring out there in a way that completely overrides the national scene. The BigTechs have an advantage due to their widespread data collection practices (which are often not in line with GDPR provisions), which national tech companies cannot compete with. Moreover, these practices are often not in line with the GDPR, making Big Tech a direct beneficiary of the enforcement gaps that are undermining the application of the regulation. Therefore, instead of focusing too much on allowing small national players to try out new technologies, one should be interested in how to avoid disasters in the BigTech sector, which is of a completely different scale.

Question 21. In your opinion, how could the relevant EU authorities enhance coordination among different schemes in the EU?

At EU level, considering the integration of the financial market and to avoid regulatory arbitrage, a certain degree of homogeneity is needed in the definition of criteria to enter the sandbox, in the internal operative and interaction with regulators and, finally, in the conditions under which the exit will take place:

- A sandbox is a specific and defined part of the market. Strict limits on the types and amounts of products that qualify should be adopted by the regulator: for instance, robo-advisers, digital currency wallets could generally be able to use the sandbox, but not lenders and FinTechs working on pensions or life insurance. In addition, a sandbox should be a closed shop for private consumers, and only open to professional consumers who are well aware of the risks involved. One of the most significant uses of digital technology which has emerged is the use of automated investment advice. While such services have the potential to increase access to financial advice for consumers, any measures to increase retail investor participation through such innovative distribution channels should be accompanied by appropriate safeguards and offered only to sophisticated consumers.
- To enter the sandbox, projects should be innovative, demonstrate the impossibility or high unlikelihood to be developed without a sandbox and provide clear benefits for the clients, following a case-by-case assessment.
- Once in the sandbox, the relevant company which must accept testing conditions that ensure no detriment to consumer rights, must prove that the proposition will not affect the open economy, and must report to the regulator according to a previously agreed roadmap.

- Exiting the sandbox is a key milestone in the process, as the final objective is that the project should enter the market under clear regulatory conditions.

Question 22. In the EU, regulated financial services providers can scale up across the Single Market thanks to adequate licenses and passporting rights.

BEUC is not opposed to extending the existing EU licences to further areas, provided that all market players are properly regulated and supervised, plus consumer access to redress mechanisms is easy and straightforward.

The growing digitalisation and online distribution of financial products means that products can be easily marketed across borders within the EU. But this is at odds with current EU rules on conduct supervision of cross-border financial firms. Currently, financial firms can obtain a license in any Member State and then passport their products and services into other EU countries through a branch or online distribution (passporting). In that case, the supervisory authority of the firm's home country is competent to oversee its activities, while the host authority (country where the firm effectively operates) has limited power over those firms. The EU passporting model does not take the consumer perspective into account and leaves room for regulatory and supervisory arbitrage, endangering market integrity and financial stability. A [report](#) on cross-border supervision of retail financial services published by the European Supervisory Authorities (EBA, ESMA, EIOPA) last year noted an increase in the number of financial services providers offering, on a cross-border basis, products not suitable for consumers. The marketing of such products is often very aggressive.

The ESAs report provided that the current passporting regime does not work well as it creates opportunities for regulatory arbitrage and forum shopping. Many financial service providers tend to obtain their passport in countries which have light licencing regimes and weak supervisors, and then can market their products to consumers abroad and escape the radar of the authorities of the consumer's country, especially when the firm operates under the 'freedom to provide services' without establishing a physical presence in the consumer's country. In this case, the respective roles of the home and host supervisors are not clearly defined, and the cooperation frameworks foreseen in sectoral financial legislation are quite inefficient due to hugely diverse quality of supervisors across Europe. This means that consumers are not well protected when dealing with foreign financial service providers operating with an EU passport.

The ESAs addressed a number of recommendations to the EU policymakers, notably:

- Consider reinforcing the harmonisation of level 1 (EU directives and regulations) provisions governing conduct of business rules in the banking sector and clearly setting out and allocating responsibilities between the home and the host competent authorities with regard to the application of consumer protection and conduct of business provisions.
- Provide more clarity on when activities carried out through digital means fall under passporting due to the lack of definition of cross-border provision of financial services and in the light of the continuing growth in the digitalisation of financial services.
- Consider clarifying the due diligence that a home competent authority should undertake prior to granting a passport.

BEUC supports the ESAs' recommendations. Furthermore, we consider that the Commission should initiate an overhaul of the passporting concept and replace it with the 'EU driving license' concept (consumer-centric approach): financial firms would still get their license in one country but would be supervised by host authorities (as per driving licenses), at least regarding firms' conduct and consumer protection in the host country. The same goes for our-of-court redress bodies: host country's ADRs should be competent to address cross-border cases.

Question 23. In your opinion, are EU level initiatives needed to avoid fragmentation in the Single Market caused by diverging national measures on ensuring non-discriminatory access to relevant technical infrastructures supporting financial services?

BEUC is very much in favour of the activities of third-party providers (TPPs) – in particular, payment initiation services providers (PISPs) regulated by PSD2. Therefore, when the discussion on the communication channel (dedicated interface or API) between banks and TPPs started in early 2017, we asked for the establishment of a single application programming interface (API) at the EU level as the only means to guarantee full reachability and interoperability among financial service providers. The work done since then has been put on hold for the time being, and the result is that each country, if not each bank, is creating its own API. Even if the majority of banks are using the Berlin Group standards, there are at the national level adaptations through the implementation rules. That triggers national fragmentation. To ensure full interoperability for TPPs, the authorities should push to a single API for the EU. This single API would also be very useful for Open Banking/Finance. It is not possible for a financial institution to adapt its IT system to the specificities of the interfaces of 4,500 banks in the EU.

Question 24. In your opinion, what should be done at EU level to achieve improved financial education and literacy in the digital context?

Financial literacy in the European Union is low, and many consumers lack the confidence and capability to make effective decisions in financial services. It is intuitive to assume that the remedy to a lack of financial literacy should be more and better financial education for consumers. However, insights from (a) behavioural economics and (b) research into the effectiveness of financial education suggest that there are significant limits in the role that education can play in improving financial outcomes for consumers. To improve financial outcomes for consumers, policymakers and regulators should focus on 'changing the offer, not the consumer'. Being a consumer should not be a full-time job, decisions in financial services should be made easier by (a) promoting product simplicity, including default options, (b) nudging consumers in the right direction (c) banning products that give rise to significant consumer protection concerns (d) increasing access to independent advice and impartial financial guidance.

It is worth adding that the issue of a digital divide between young and elderly people is unlikely to disappear, due to age-related sensorial, cognitive and physical declines as well as health issues.

In addition, the increased digitalisation of financial services risks adding further complexity for financial services users in certain regards. Understanding how digital financial services work and the potential consequences that consumers could face, for example, through the (mis)use of personal data may not be easy for certain segments of consumers to understand. The emergence of new players with new practices and different business models could add to the complexity in financial services. As a result, ensuring that new digital financial services firms are adequately regulated and supervised becomes even more critical for consumers.

Question 25: If you consider that initiatives aiming to enhance financial education and literacy are insufficient to protect consumers in the digital context, which additional measures would you recommend?

Financial products are often complex, or frequently unsuitable for meeting most consumer needs. Consumers do not necessarily need more choices in financial services, but better choices. BEUC favours the establishment of simpler financial products for financial consumers with uncomplicated and standardised features and encourages the use of default options and/or standardised features in the most common financial products. Transparent, standardised products that enhance comparability for consumers can increase consumer trust in financial services products. BEUC supports the European Parliament's call in its Report on the Action Plan on Retail Financial Services for the European Commission "to look into the possibility of creating a harmonised legal framework for standardised default options for the most commonly used EU financial products, along the lines of the Basic Bank Account and PEPP model." A recent European Commission behavioural study on the digitalisation of the marketing and distance selling of retail financial services also recommended the development of simpler financial products (recommendation 3). As an example, BEUC supports the recent EU agreement to establish a pan-European Pension Product, which will require all future PEPP providers to offer a cost-efficient and safe Basic PEPP (representing the default option suitable for most pension savers).

Question 26: In the recent communication "A European strategy for data", the Commission is proposing measures aiming to make more data available for use in the economy and society, while keeping those who generate the data in control?

BEUC agrees that promoting measures to make financial data more accessible can result in benefits for consumers. However, rules are needed to ensure that consumers can remain in control of their data. The consumer should always be able to decide who gets access to his or her personal data and under what conditions. Overruling this active role of the consumer should be limited to exceptional cases established in the law. In particular, EU rules on accessing and sharing data must²:

- Ensure that consumers are adequately protected against data breaches, misuse of data, privacy and security risks associated with the sharing of consumers' financial data. Regulation must be adopted to ensure that consumers' data is used in full respect of data protection legislation and consumers' rights, and that liability is clear in case things go wrong.

² For more information on our position on the European Data Strategy please see BEUC response to the Commission's public consultation on this topic.

- Consumers should have a right to instruct financial services providers (the data guardian) not to share their data with third parties.
- Consent should be freely and voluntarily given by the consumer and should not be extorted from the data subject by conditioning access to essential services or products on accepting the privacy policy.
- Data should not be accessed without the explicit consent of the consumer. Explicit consent under PSD2 should be held up to the same high standards as explicit consent under the GDPR.
- Consumers must be able to easily keep track of and control who they have granted consent/access to, and the financial institution should maintain a list of all third parties that have access to the consumer's financial data. As for the direct debits, the consumer should be able to ask the financial institution to establish a white list (AIS who can have access) and a blacklist (AIS which are not accepted).
- The consumer should be able to give their consent to certain types of data being shared, but not all (for instance, a consumer may wish to share their savings account information, but refuse to share payment account information). When the consent is given by a consumer to a third party, the financial institution (as the guardian of the data) should be informed by the third party as to which data the access agreement has been given; the financial institution should verify with the consumer what data they have given access to and set up the access in conformity with the choice of the consumer.
- The consumer should be able to cancel at any time any specific agreement that they have given to a third party, and there should be a clear right for consumers to be forgotten. The consumer should be able to cancel any specific agreement that he or she has, either through the third party, or through the data guardian (i.e. the bank or insurance company)
- Financial authorities must be able to scrutinize the data sharing systems to ensure compliance with consumer, competition and data protection rules.

Question 27. Considering the potential that the use of publicly available data brings in finance, in which areas would you see the need to facilitate integrated access to these data in the EU?

BEUC supports the creation of an EU-wide database to facilitate easier comparison by retail investors between different types of investment products. At the moment, no such EU-wide database exists. In 2019, the European Supervisory Authorities published reports into the cost and performance of retail investment products. The ESAs faced considerable difficulties in gathering and aggregating data on the products under their supervision and relied on information provided through commercial databases or in cooperation with market participants to carry out their analysis. The creation of an EU-wide database on investment products could assist the ESAs in monitoring the cost and performance of products under their supervision.

In addition, the creation of an EU-wide database could facilitate the emergence of independent comparison tools or price comparison websites for consumers, allowing them to easily compare the costs and features of investment products. As an example, in Norway, financial institutions are required under Norwegian law to provide price and other information to our member Forbrukerrådet in order to operate an independent comparison tool (finansportalen.no) that covers investment funds, life insurance and private pension products. Comparison tools could assist retail investors to compare between providers and the key features of investment products (including cost, risk, etc.). Independent comparison tools can also give retail investors an overview of the available product providers on the market.

As demonstrated by the European Commission's [Retail Distribution Study](#) (p.78), retail investors struggle to collect comprehensive information on the fees of investment products, impeding their ability to compare between different products and distributors. Often, consumers need to talk directly with an adviser in order receive necessary information to understand the cost of investment products. It can also often be difficult to find the relevant disclosure documents on the website of providers (such as the PRIIPs or UCITS KID). This in turn increases efforts for retail investors to compare products and distributors. As a result, the Retail Distribution Study concludes that retail investors might simply refrain from investing or simply choose among the products provided by the bank or insurance company where they are already a client, preventing them from shopping around. Independent comparison tools could assist retail investors to compare different providers on the market and shop around, in turn improving competition between different providers.

The creation of an EU-wide database on investment products could also facilitate the emergence of better disclosure for retail investors and allow new tools to be developed for consumers to compare the features of investment products. In 2018, the UK Financial Conduct Authority published a [discussion paper](#) on 'drawing attention to charges in the asset management industry'. The paper drew attention to the fact that simply providing consumers with information in disclosure documents about charges, does not guarantee that they will use it in their decision-making. The paper found that clearly presenting engaging information in a prominent way can enhance the effectiveness of disclosures. For instance, the paper found that using colour, graphics and plain language as well as warnings and impact charts helped consumers in their decision-making when making investment decisions. In the United States, FINRA already operates a 'Fund Analyzer' tool that allows retail investors to compare investment funds.³ Similar comparison tools could allow European consumers to compare the core features of investment products offered to them by advisers and could be signposted in relevant disclosure documents provided to retail investors (such as the PRIIPs KID, the UCITS KIID document, ex-post MiFID II costs disclosures, etc.).

Question 29. In your opinion, under what conditions would consumers favour sharing their data relevant to financial services with other financial services providers in order to get better offers for financial products and services?

The increased use of data and technology is changing how financial markets work for firms and consumers. The Payment Services Directive (PSD2) first introduced a legal environment enabling consumers to consent to third parties accessing their payment account information and established clear technical rules for accessing this consumer data. The scope of PSD2 is currently limited to payment accounts, and at the moment does not cover savings accounts, investment accounts, pensions savings, mortgages and consumer

³ https://tools.finra.org/fund_analyzer/

credit, or insurance products. Sharing non-payment account information and broadening the scope of account data could have benefits for consumers. Open Finance could make it easier for consumers to receive proposals to compare the costs and product features and switch between providers, in turn improving competition between financial services providers as well as spurring the creation of innovative new services or tools for consumers. Open Finance could stimulate the provision of financial products by non-bank third parties (such as FinTech firms or other product providers) and other banks acting as 'third parties' in turn stimulating competition between firms. However, there are several potential risks associated with the increased sharing of consumer data, that deserve scrutiny and adequate safeguards for consumers. To ensure that Open Finance is implemented in a consumer-friendly way, several safeguards or principles should be adopted.⁴

See also answers to question 1 and 26.

Question 31. In your opinion, what could be the main risks of implementing an open finance policy in the EU?

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Privacy issues / security of personal data	●	●	●	●	X	●
Financial exclusion	●	●	●	●	X	●
Poor consumer outcomes (e.g. unfair pricing strategies)	●	●	●	●	X	●
Misuse of consumers' financial data	●	●	●	●	X	●
Business confidentiality issues	●	●	●	●	●	X
Increased cyber risks	●	●	●	●	X	●
Lack of level playing field in terms of access to data across financial sector activities	X	●	●	●	●	●

⁴ For more information, please see our position paper on consumer-friendly open banking, 20.09. 2018: https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf

Other	<input type="radio"/>						
-------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Question 32. In your opinion, what safeguards would be necessary to mitigate these risks?

Opening access to consumer data could lead to an increased risk of fraud, necessitating the creation of adequate security standards when third parties access consumer data. Under PSD2, banks have set up common and secure open standards of communication (referred to as Application Programming Interface standards) between them and third parties wishing to access the consumer data. However, where third parties are unable to access consumer data through an API, they employ so-called 'screen scraping' techniques to access consumer data.

Screen-scraping raises serious security and consumer protection risks that should be addressed through legislation. Such techniques are unsecure for the consumer since it requires the sharing of a consumer's personal security credentials (such as their PIN information) with third parties. Furthermore, screen-scraping gives third parties full access to the customer's account, including for example, the ability to access data that has not been fully authorised by the consumer.

Stricter authorisation methods through an API provide more control over the type and extent of data that is shared with third parties and offers a more secure way to interact with third parties. Technical solutions exist in order to avoid the communication of sensitive consumer information with third parties and must be adopted to ensure secure communication between consumers, firms and third parties. Third parties should only be allowed to access consumer data through the so-called re-direction authentication method, to ensure that consumer's personalised security credentials (such as their PIN information) are not shared with any third parties.

Wider access to consumer data by third parties must take place in a safe and properly regulated environment, with the informed explicit consent of the consumer. Open Finance must be based on the principle that the data supplied by and created on behalf of financial services consumers must remain under the full control of those consumers. Data should not be accessed without the explicit consent of the consumer. It should be clear to consumers who they are giving consent to for accessing their data and for what purposes. Consent should not be a routine 'tick the box' exercise, but based on the informed and explicit consent of the consumer [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 (bank) "YYY"]. Collecting data about credit and debit card transactions can reveal sensitive information about the health, sexuality, religion, political views or other personal details of a person. The legislation should guarantee that third parties only have access to data that are necessary for their activity, and clear restrictions are needed on further sharing such data or reselling customer data for purposes beyond the customer's initial consent. The wider sharing of data with more parties also raises the risks of a data breach or misuse of data occurring, and clear rules are needed to assign liability in the event of financial loss, erroneous sharing of sensitive data, or other data breaches.

Consumers need to be adequately protected against data breaches, misuse of data, privacy and security risks associated with the sharing of consumers' financial data. Regulation must be adopted to ensure that consumers data is used in a fair and lawful manner and that liability is clear in case things go wrong. Consumers should have a right to instruct their

bank not to share their data with third parties. Data should not be accessed without the explicit consent of the consumer. Consumers must be able to easily keep track of who they have granted consent/access to, and the consumer's bank should maintain a list of all third parties that have access to the consumer's financial data. The consumer should be able to give their consent to certain types of data being shared, but not all (for instance, a consumer may wish to share their saving account information but refuse to share payment account information). When the consent is given by a consumer to a third party, the bank (as the guardian of the data) should be also informed as to which data the access agreement has been given; and set up the access in conformity with the choice of the consumer. The consumer should be able to cancel at any time any specific agreement that he or she has given to a third party, and there should be a clear right for consumers to be forgotten. The consumer should be able to cancel any specific agreement that they have, either through the third party, or through the data guardian (i.e. the bank).

In addition, while Open Finance could benefit digitally active consumers, there is also a need to ensure that relevant products and services remain accessible for non-digital clients.

Question 33. In your opinion, for which specific financial products would an open finance policy offer more benefits and opportunities?

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Savings accounts	●	●	●	●	X	●
Consumer credit	●	●	●	●	X	●
SME credit	●	●	●	●	●	X
Mortgages	●	●	●	●	X	●
Retail investment products (e.g. securities accounts)	●	●	●	●	X	●
Non-life insurance products (e.g. motor, home...)	●	●	●	●	X	●
Life insurance products	●	●	●	●	X	●
Pension products	●	●	●	●	X	●
Other	●	●	●	●	X	●

If you see other financial products that would benefit of an open finance policy, please specify and explain:

Payment services. It is in the payments sector that the competition between Big Tech and incumbents will be the more intense. It is important to keep in mind that, according to PSD2, credit institutions (banks) have access to the accounts consumers hold in other banks, without asking for a specific license. Other institutions need a specific license. In 2019, Dutch banks were told to stop using their customers' payments data for the purposes of personalised direct marketing. The Dutch Data Protection Authority has explained: "Payment data gives a complete picture of someone's life: what do you spend your money on, which associations do you belong to, who do you associate with."

Question 34. What specific data (personal and non-personal) would you find most relevant when developing open finance services based on customer consent?

In recent years, several BigTech companies have established payment subsidiaries (such as Apple Pay or Google Pay). In line with PSD2, these subsidiaries are classified as payment institutions or 'e-money' institutions. This gives them the ability to access the consumer data held by banks. The banking industry now argues that if third parties have access to the data they hold on consumers, banks should have in return access all types of data that GAFA and other technology companies hold about consumers (i.e. 'reciprocity').

However, BEUC believes that reciprocity is unacceptable for several reasons (see our factsheet [here](#)):

- **Risks for consumers' control over their personal data.** Consumers might have a fair idea about what their bank knows about them, but much less so when it comes to third parties like BigTechs. These companies know much more about consumers than banks, often collecting and combining data related to all aspects of a consumers' life. Through geo-location, for example, about the places a person has visited; their sporting or leisure habits; data about friendship networks, chat history, opinions and beliefs or even online search and browsing history. Consumers are often not aware of how much data these companies have about them (which is already problematic on its own). Reciprocity means consumers would be asked to give their banks access to all kinds of personal data, perhaps unaware about what they are giving access to. It is also unclear how such personal information could help banks and other financial institutions improve their services and why it would be necessary to grant such access. At a time when consumers need more control over their personal data, reciprocity would mean greater risks and less control from a consumer data protection perspective.
- **Consumer consent needs to be reinforced.** Existing means to obtain valid consumer consent are insufficient. Users tick a cookie box to access a website, for example, without any idea of the consequences of this agreement. When granting banks access to personal data held by other companies, consumers would find themselves in a similar situation. For a start, their consent cannot be considered meaningful and informed when they are not aware of which data they would be giving access to and of the consequences. Consumers might also be 'forced' to give blanket access to all their data held by a company, without any choice or sufficient transparency as to the purpose. This is not an issue exclusive to reciprocity, but it becomes even more problematic given the sensitivity of the financial services area.

That is why it is necessary to review the conditions in which consumers can validly consent to enable access to this data.

- **No market failure.** Reciprocity makes sense for financial data (or non-financial data necessary to provide a financial service). But it cannot extend to non-financial data that are not necessary to provide a financial service. Banks' request to extend reciprocity to these types of data (e.g. your shopping habits, your friends, your movements) is not justified by any market failure. This is because banks *can* still provide the service without such extensive consumer profiling.

In the case of the GAFA, there is a need to guarantee that data collected by a payment subsidiary are not provided to or merged with the data held by the parent company (there is a need for 'Chinese walls' between the payment subsidiary and the parent company). Lastly, where firms rely on datasets that combine personal and non-personal data, access to the whole data set should be governed by the rules of the GDPR.

Question 35. Which elements should be considered to implement an open finance policy?

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Standardisation of data, data formats	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Clarity on the entities covered, including potential thresholds	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Clarity on the way data can be technically accessed including whether data is shared in real-time (e.g. standardised APIs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>

Clarity on how to ensure full compliance with GDPR and e-Privacy Directive requirements and need to ensure that data subjects remain in full control of their personal data					X	
Clarity on the terms and conditions under which data can be shared between financial services providers (e.g. fees)					X	
Interoperability across sectors	X					
Clarity on the way data shared will be used					X	
Introduction of mandatory data sharing beyond PSD2 in the framework of EU regulatory regime					X	
If mandatory data sharing is considered, making data available free of cost for the recipient					X	
Other						

Please specify what other element(s) should be considered to implement an open finance policy:

Application Programming Interface (API) standards are a set of rules and specifications used between banks and third parties to communicate using the same set of communication protocols, security profiles and data standards. However, since the entry into force of PSD2, a large variety of different API standards exist across Europe, meaning that third party firms may need to use different API standards to communicate with different banks. This leads to challenges, such as inefficiencies for third parties wishing to access banking data and the fragmentation of the digital financial ecosystem. The development of API standards should be done in a way that promotes interoperability, efficiency and usability for all users. The European institutions should support the development of a single EU-wide Application Programming Interface (API) for the purposes of PSD2 and for any future initiatives in Open Finance. See also our response to Q23.

Question 39. In your opinion, what are the main challenges or risks that the increased use of AI- based models is likely to raise for the financial industry, for customers/investors, for businesses and for the supervisory authorities?

- **For consumers/investors:**

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
2.1. Lack of awareness on the use of an algorithm	●	●	●	●	X	●
2.2. Lack of transparency on how the outcome has been produced	●	●	●	●	X	●
2.3. Lack of understanding on how the outcome has been produced	●	●	●	●	X	●
2.4. Difficult to challenge a specific outcome	●	●	●	●	X	●
2.5. Biases and/or exploitative profiling	●	●	●	●	X	●

2.6. Financial exclusion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
2.7. Algorithm-based behavioural manipulation (e.g. collusion and other coordinated firm behaviour)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
2.8. Loss of privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
2.9. Other	<input type="radio"/>					

Please specify what other main challenge(s) or risk(s) the increased use of AI-based models is likely to raise for customers/investors:

The use of Artificial Intelligence is set to profoundly change the way financial services products are designed, marketed and sold to consumers. While such evolutions come with potential benefits for users, including potentially better targeted offers for certain segments of consumers, it equally raises concerns related to the protection of user data, privacy, fairness, freedom of choice, and financial exclusion. New legal safeguards are needed to ensure that AI benefits consumers and does not harm them. For instance, in the area of insurance, BEUC sees several risks for consumers, including new forms of financial exclusion and price optimisation techniques employed by insurance firms.

- **For supervisory authorities:**

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
3.1. Lack of expertise in understanding more complex AI-based models used by the supervised entities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
3.2. Lack of clarity in explainability requirements, which	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>

may lead to reject these models						
3.3. Lack of adequate coordination with other authorities (e.g. data protection)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
3.4. Biases	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
3.5. Other	<input type="radio"/>					

Please specify what other main challenge(s) or risk(s) the increased use of AI-based models is likely to raise for the supervisory authorities:

The use of AI by firms will need to be closely monitored by supervisors. In particular, the use of personal data and the output of AI/ADM systems must be thoroughly and independently monitored by public authorities to ensure that consumers are not unfairly discriminated against when taking out financial services products. Supervisors will need to regularly audit algorithms to detect potentially unlawful discriminatory outcomes. For AI applications to be considered highly risky, ex-ante regulatory intervention should be envisaged before market deployment. According to a survey by our German member vzbv, nearly 80% of consumers said that supervisory authorities should be able to check whether automated decisions comply with applicable laws.

Question 40. In your opinion, what are the best ways to address these new issues?

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
New EU rules on AI at horizontal level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
New EU rules on AI for the financial sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Guidance at EU level for the financial sector	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Experimentation on specific AI applications under the control of competent authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>	<input type="radio"/>

Certification of AI systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Auditing of AI systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Registration with and access to AI systems for relevant supervisory authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Other	<input type="radio"/>					

Please specify what other way(s) could be best to address these new issues:

A horizontal legal framework should be adopted setting out the main principles to regulate AI and ADM systems and ensure fairness, transparency, accountability and control (see our position paper on '[AI Rights for Consumers](#)'). New regulations should follow the general principle that the higher the potential adverse impacts of the use of algorithmic decision making and AI technology, the stronger the appropriate regulatory response must be. In the area of financial services, especially in insurance and lending, the risks for consumers could be especially high, and specific new rules on AI need to be adopted to ensure that insurance consumers and borrowers do not face discrimination or potential consumer harm. Please see BEUC's [position paper](#) on the use of Big Data and AI in insurances for our full recommendations.

END



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

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.