

The Consumer Voice in Europe

## EIOPA DISCUSSION PAPER ON OPEN INSURANCE: ACCESSING AND SHARING INSURANCE-RELATED DATA

BEUC response



**Contact: Jasper De Meyer – [financialservices@beuc.eu](mailto: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](http://www.twitter.com/beuc) • [www.beuc.eu](http://www.beuc.eu)  
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2021-041 - 05/05/2021

## Why it matters to consumers

Open Insurance initiatives that allow consumers to share their insurance-related data with third parties based on their explicit consent could help to deliver new innovative services for consumers and allow them to more seamlessly compare and switch between insurance products. However, efforts to develop an EU-wide Open Insurance initiative should not come at the expense of consumers losing control over their personal data, suffering the consequences of illegitimate data processing, ubiquitous profiling and discriminatory practices or financial exclusion. Strong consumer protections and regulatory safeguards are required to ensure that Open Insurance initiatives work in the best interest of consumers.

## Summary

---

Data and technology are changing how financial markets work for consumers. Open Finance initiatives have the potential to deliver better financial products and services to consumers, while improving competition between financial firms. Access to and the sharing of insurance-related based on the explicit consent of the consumer could help consumers to compare and switch more seamlessly between insurance products, while helping to deliver innovative new services for insurance consumers.

However, sharing data with third parties can often reveal very sensitive information about consumers. In a sensitive area such as financial services, consumers may particularly be unaware of the consequences of agreeing to share personal information about themselves with third parties, and sharing such data may not always be in their best interest. A consumer's focus on buying an insurance product may also mean that other important considerations, such as their privacy, data protection and security concerns, may feature less prominently in their decision making.

An EU-wide Open Insurance initiative would extend Open Banking principles to a wider range of a consumer's financial data, including information related to consumers insurance policies and their pension savings. BEUC believes that extending Open Banking principles beyond payment accounts to the insurance sector should only be considered if it is accompanied with:

- (a) Strong consumer protections;
- (b) Stricter data protection provisions;
- (c) Better data consent management tools for consumers; and
- (d) Clearer rules about what types of data can be considered about consumers in the pricing and risk assessment processes of insurance firms.

**1. Do you agree with the definition and the approach to open insurance highlighted in the Discussion Paper? If not, please describe what aspects would be essential to consider additionally?**

- **Yes**
- No
- I don't know

**2. In addition to those described in this paper, including in Annex 1, do you see other open insurance use cases or business models in the EU or beyond that might be worth to look at further from supervisory/consumer protection perspective?**

- Yes
- **No**

**3. Do you think regulators/supervisors should put more focus on public comparison websites where the participation is compulsory for undertakings? What lines of business could be subject for that? What risks, benefits and obstacles do you see?**

Yes.

Public independent comparison tools can play an important role in helping consumers to compare between insurance products, enhancing consumer access to information and supporting their decision making in finding the best deal. We support further focus on making public independent comparison tools more widely available to consumers in retail financial services (including for insurance and pension products). We note that there are already existing initiatives in certain retail financial services markets to facilitate access to comparison tools for EU consumers:

For instance, under Article 7 of the Payment Accounts Directive, EU Member States are required to ensure that consumer have access, free of charge, to at least one website comparing the fees charged by payment service providers for payment accounts. The comparison website can be operated by a public authority or a private operator, but must comply with certain criteria (such as being independent, and making sure that payment service providers are given equal treatment in search results). Similar requirement under sectorial financial services legislation (including in insurances, pensions, investments, etc.) could be envisaged to help consumers to compare the key features and costs of retail financial services products.

Several of our member organisations also offer independent comparison tools for consumers in their countries. For instance, in Norway, the Norwegian Consumer Council operates an independent comparison tool called Finansportalen for retail financial services products, including bank accounts, life insurance policies, investment funds, pension products and other insurance policies (such as car insurance, home insurance, and travel insurance). Under Norwegian law, it is mandatory for financial services providers to disclose information in a prescribed format to the Finansportalen website for the basis of building the comparison tool.<sup>1</sup> Studies by our member show that the Finansportalen website contributes to the financial education of consumers in Norway. According to our Norwegian member, approximately 1.3 million people use Finansportalen per year. As of 2018, surveys show that 34% of male citizens and 42% of female citizens in Norway have knowledge of it.

---

<sup>1</sup> Finansportalen, 'About Finansportalen', <https://www.finansportalen.no/andre-valg/om-finansportalen/>.

**4. Please describe your own open insurance use case/business model and challenges you have faced in implementing it, if any.**

No comments.

**5. In addition to those described in this paper, do you see other open insurance use cases in RegTech/SupTech that might be worth to look at further from supervisory/consumer protection perspective?**

The development of an Open Insurance framework could open doors to new supervisory tools for financial supervisors, and BEUC supports several of the use cases described in EIOPA's discussion paper. In particular, the development of machine-readable key information documents (such as the PRIIPs Key Information Document) could support market monitoring from a conduct of business perspective. While PRIIP KIDs are publicly available documents, there is currently no obligation for such information to be provided to consumers in a centralised place. The documents are generally also published in a PDF format, making it difficult for financial supervisors or other interested stakeholders to extract information from them and challenging to use in a supervisory context.

We believe that Key Information Documents could benefit from further standardisation and digitalisation, including requiring such documents to be made available in a machine-readable way. The European Securities and Markets Authority (ESMA) recently published a study into the potential SupTech applications associated with analysing PRIIPs KID information. The study includes a recommendation that "when a law requires the widespread production of documents, it is essential that these be made available in a flexible format such as open document format, even if in addition to PDF."<sup>2</sup> The European Commission has also published a study on the potential development of an online repository or database containing complete, correct and independent information on all managed financial products available across EU capital markets.<sup>3</sup>

**6. Please describe your own open insurance use case/business model in RegTech/SupTech and the challenges you have faced in implementing it, if any.**

No comment.

**7. Do you you agree the potential benefits for the consumers are accurately described?**

- Strongly agree
- **Somewhat agree**
- Neither agree nor disagree
- Strongly disagree

**8. Are there additional benefits?**

BEUC recognises the potential benefits identified by EIOPA that could emerge for consumers from the development of Open Insurance solutions. Wider sharing of the data based on the explicit consent of the consumer could make it easier for consumers

---

<sup>2</sup> ESMA, 'Trends, Risks and Vulnerabilities', '54,000 PRIIPs KIDs – how to read them (all)', [https://www.esma.europa.eu/sites/default/files/library/esma50-165-1524\\_trv\\_1\\_2021.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-165-1524_trv_1_2021.pdf)

<sup>3</sup> European Commission, 'Study on options for development of online tools and services supporting retail investors in investment decisions', <https://op.europa.eu/en/publication-detail/-/publication/74844f7c-cbc7-11ea-adf7-01aa75ed71a1/language-en/format-PDF/source-140558169>

to compare the price and product features of financial services providers, facilitate simpler on-boarding for consumers, increase competition by making it easier for consumers to compare the market and compare between providers, and boost competition by facilitating the entry of new firms into the market providing financial services.

## 9. What can be done to maximise these benefits?

We believe that consumers can benefit from the increased digitalisation of financial services and the emergence of Open Finance initiatives. While the objective of increased competition between financial services providers can improve consumer welfare in financial services markets, it will not do so if consumers lose control over their personal data and suffer the consequences of illegitimate data processing, ubiquitous profiling and discriminatory practices. To ensure that the benefits of Open Finance initiatives can be maximised, a consumer-focused approach is required, and should be based on the following principles elaborated by our member Which?<sup>4</sup>:

- Open Finance initiatives should be a force for good which promotes financial inclusion and widens access to more useful, affordable and understandable financial services for everyone.
- Services should meet people's positive expectations, be upfront about how they're paid for and how they use personal data. They should be sold and delivered in a way that respects people's identity, their data and their right to make the most of their money and lead the lives they want to.
- Open Finance initiatives should genuinely equip people with real power to control access to their account and use of their data. People should be able to stop sharing access to their account easily without facing penalties.
- Open Finance initiatives should be reliable and as secure as it possibly can be. It should be clear to people with whom they are sharing their data and the legitimacy of these companies. Data breaches and fraud should be rare and exceptional, not the rule. Where data breaches occur, consumers should be compensated.
- People, their identity and their money should be universally safe. People should not bear unfair risk. When things go wrong, people should have simple, free, quick access to help and redress.

## 10. Do you agree the potential risks for the consumers are accurately described?

- Strongly agree
- **Somewhat agree**
- Neither agree nor disagree
- Strongly disagree

## 11. Are there additional risks?

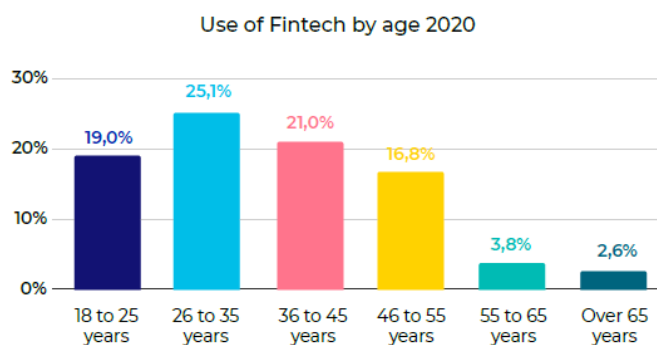
BEUC sees the following main risks associated with the development of any Open Insurance framework:

**Risk of exclusion:** The development of an Open Insurance framework could lead to the exclusion of non-digital consumers, who may struggle to access such services and be unable to access better prices offered through new business models associated with Open Insurance initiatives. According to our member Which?, "a fifth of consumers in the UK do not use online banking, with a similar amount who are not confident they

---

<sup>4</sup> Which?, 'Response to FCA call for input: Open Finance', [https://about-which.s3.amazonaws.com/policy/media/documents/603e63fe4ab89-Which\\_%20%20Response%20-%20Open%20Finance%20Call%20for%20input%20\(1\).pdf](https://about-which.s3.amazonaws.com/policy/media/documents/603e63fe4ab89-Which_%20%20Response%20-%20Open%20Finance%20Call%20for%20input%20(1).pdf).

could check their balance online. When it comes to other offerings, around two-fifths of consumers would not feel confident making a query on a chat tool or applying for a loan or credit online. There are concerns that these consumers will struggle to use and benefit from Open Finance tools and services.” Evidence from a study<sup>5</sup> by our Spanish member ASUFIN likewise demonstrates that the use of FinTech services often differs significantly between age groups, with elderly groups among those least likely to rely on such services:



There is a risk that the benefits of innovative new services provided to consumers will be limited to the tech-savvy, with other customers potentially losing out if they do not engage with such data-sharing initiatives. Already there is evidence in several markets, including in the United Kingdom<sup>6</sup> and Ireland<sup>7</sup>, that insurance firms often engage in price optimisation practices to the detriment of certain segments of consumers. A study by the UK’s Financial Conduct Authority found that insurance firms were more likely to target price increases on consumers who were perceived as less likely to switch between insurance providers, and that vulnerable consumers (such as the elderly and/or consumers with lower financial capabilities) often paid higher premiums compared to consumers who regularly switched insurance providers. Such trends could be exacerbated by the emergence of any Open Insurance initiatives and should be carefully monitored. All consumers need to be considered in any eventual Open Insurance framework, including those who could be excluded from a market because of having certain characteristics (such as having lower digital skills, or lower financial capabilities, or consumers lacking access to the internet).

**Inadequate consent management:** Current means to obtain consumer consent are often completely inadequate and too complex for consumers. Too often personal data protection depends on the assumption that consumers are fully aware of the processing activities, can read and understand long and complex privacy policies. Data held by financial services firms can reveal very sensitive information about the health, sexuality, religion, political views or other personal details of a person. In a sensitive area such as financial services, consumers may particularly be unaware of the consequences of agreeing to share personal information about themselves with third parties. A consumer’s focus on buying an insurance product may mean that other

<sup>5</sup> ASUFIN, ‘Study about the knowledge, habits and use of FinTech in Spain’, [https://www.asufin.com/wp-content/uploads/2020/12/2020\\_II\\_STUDY\\_ABOUT\\_KNOWLEDGE\\_HABITS\\_AND\\_USE\\_OF\\_FINTECH\\_IN\\_SPAIN.pdf](https://www.asufin.com/wp-content/uploads/2020/12/2020_II_STUDY_ABOUT_KNOWLEDGE_HABITS_AND_USE_OF_FINTECH_IN_SPAIN.pdf).

<sup>6</sup> Financial Conduct Authority, ‘General insurance pricing practices – interim report’, <https://www.fca.org.uk/publication/market-studies/ms18-1-2-interim-report.pdf>.

<sup>7</sup> Central Bank of Ireland, ‘Review of Differential Pricing in the Private Car and Home Insurance Markets’, <https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/insurance-reinsurance/solvency-ii/communications/review-of-differential-pricing-in-the-private-car-and-home-insurance-markets.pdf?sfvrsn=6>.

important considerations, such as their privacy and security concerns, may also feature less prominently in their decision making.

- For instance, a study<sup>8</sup> by the UK's Financial Services Consumer Panel (FSCP) shows that consumers who relied on Open Banking services often did not read the full terms and conditions, because they were too long and complicated, full of legal jargon, and often not written with the consumer in mind. Although consumers often expressed their concerns about sharing their data with financial services providers, speed and convenience were often overriding factors in deciding whether to sign up for an application or a service.
- A study<sup>9</sup> by our member vzbv shows that while the implementation of the PSD2 has resulted in concrete benefits for consumers (new tools help consumers to keep track of their finances, greater choice of payment methods, better switching services for consumers, and increased competition between financial services providers), concerns have emerged in Germany in relation to data protection and inadequate protection of consumer privacy. Sensitive data held by consumers is often too easily shared with third parties (without the explicit consent of the consumer) and data processing by Open Banking apps is often very extensive (beyond what is necessary to provide the service to the client, including for instance processing that consumers would not normally expect from a payment initiation service).

Rules to obtain consumer consent under Open Finance initiatives should be strongly reinforced, and we believe that any initiatives to extend PSD2-type sharing of data to other financial services sectors should be preconditioned on adopting stricter consent management rules and stricter data protection requirements. It would be desirable to develop a clear framework of data rights around the giving and withdrawing of consent for users of Open Finance initiatives (see our detailed proposals in Question 12).

**Misuse of data:** The risk of data misuse, financial crime, fraud or scams could be greatly increased if personal data is more widely shared with insurance firms and/or other third parties. There is a risk of third parties obtaining unauthorised knowledge about aspects of consumer's life, including potentially very sensitive data, which pose risks for consumers if such data were shared with other parties.<sup>10</sup> Stricter rules are needed to ensure that data is not misused, and that consumers have a right to redress in case of data breaches.

**Surveillance society:** The growing use of data by insurance firms also trigger questions about the possible discrimination of privacy-minded consumers. The increased use of personal data and telematics-based monitoring in insurance could become very intrusive in people's personal lives, dictating how they drive, what they eat, how many daily steps they should take. Business models based on digital monitoring that reward or penalise certain lifestyle choices or behaviour that are deemed 'good' or 'bad' by an insurance firm could be considered very intrusive, paternalistic, or interfering with an individual's independence and freedom in his or her decision-making. In future, consumers may increasingly be expected or even required to undergo intrusive monitoring processes when accessing insurance. Such intrusiveness would be considered particularly problematic if individuals were unable to access insurance without agreeing to mandatory monitoring of their behaviour. Consumers who choose to opt out of data sharing arrangements due to privacy

---

<sup>8</sup> Financial Services Consumer Panel, 'Consenting adults? Consumers sharing their financial data', <https://www.fs-cp.org.uk/press-release-consenting-adults-consumers-sharing-their-financial-data>

<sup>9</sup> Vzbv, 'Offene Flanke beim Open Banking', <https://www.vzbv.de/pressemitteilung/offene-flanke-beim-open-banking>.

<sup>10</sup> Which?, 'Cybercriminals selling data breach victims' stolen data on the dark web, Which? reveals', <https://press.which.co.uk/whichpressreleases/cybercriminals-selling-data-breach-victims-stolen-data-on-the-dark-web-which-reveals/>



concerns may also face future financial exclusion. Equally, there is a risk that privacy-minded consumers could get less advantageous premiums when purchasing insurance contracts compared to consumers willing to forego privacy concerns. Excessive differentiation in pricing based on a consumer's willingness to share data with insurers could be tantamount to levelling a 'privacy premium'. In the future, consumers may find it increasingly difficult to avoid opting in due to the financial disadvantages in doing so, and users may have no option but to hand over access to their data for accessing insurance. Consumers who choose not to allow their data to be shared with insurers could face restricted access, be required to pay higher premiums, or otherwise be excluded from taking out insurance contracts.

**12. Do you you consider that the current regulatory and supervisory framework is adequate to capture these risks? If not, what can be done to mitigate these risks?**

- Yes
- **No**
- I don't know

The current regulatory and supervisory framework is not adequate to capture the potential risks emerging from Open Finance initiatives. Any extension of Open Finance initiatives beyond the current PSD2 requirements should only be considered if such reforms are accompanied with a clear set of consumers rights and better rules to ensure that consumer's data protection is fully guaranteed. We believe that the following rights and safeguards are critical for consumers:

- Consent should not be a routine general 'tick the box' exercise. Wider access to consumer data by third parties must take place in a safe, legal and ethical environment, with the informed and 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 fully controlled by those consumers.
- Consent should be freely given, specific, informed, explicit and unambiguous. In BEUC's view, consent cannot be regarded as 'informed' when it is based on long and complex contractual terms and conditions and privacy notices that are frequently not read or understood by consumers.
- Consent should be granular and specific. 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 insurance account information with a third party, but refuse to share their pension 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; and 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.
- 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. It should be clear to consumers who they are giving consent to for accessing their data and for what purposes. It should be presented to the consumer in a very clear manner, separate from other issues. For example: ['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 (insurer) "YYY"'].<sup>11</sup>

---

<sup>11</sup> For our full recommendations on consumer consent in Open Banking, please refer to section 5 of our [position paper](#) on Open banking.



- User interfaces to obtain consent should not include 'dark patterns' or other techniques to manipulate and/or influence their decisions, nudging them into giving their consent.<sup>12</sup> Through so-called 'dark patterns' or deceptive design practices, consumers are often nudged towards making choices that are in the interest of the service provider, but potentially against their own interests.
- Data held by financial services providers 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 its activity, and clear restrictions are needed on sharing such data with fourth parties or reselling customer data for purposes beyond the customer's initial consent.<sup>13</sup>
- It should be as easy to withdraw consent, as it was to give it in the first place. Consumers should benefit from practical consent management tools where they can see to whom they have given access to their data and easily revoke their consent. Consumers need meaningful options to control their data and all the parties who may have access to it. Consumers should have a right to instruct financial services providers (the data guardian) not to share their data with third parties. 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. 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.
- Consumers should be adequately protected against data breaches, misuse of data, privacy and security risks associated with the sharing of consumers' financial data. There should be a clear route to complaints for consumers, including access to redress and compensation case of any potential data breaches.

Lastly, we believe that increased cooperation between data protection authorities and financial supervisors is fundamental to the functioning of any future initiatives in Open Finance. Strengthened and structured cooperation between data protection and financial services regulators should be a pre-condition for the establishment of future Open Finance initiatives.

### 13. Do you agree with the barriers highlighted in chapter 5?

- Strongly agree
- Somewhat agree
- **Neither agree nor disagree**
- Strongly disagree

### 14. What additional regulatory barriers do you see?

No comment.

---

<sup>12</sup> Forbrukerrådet, 'Deceived by design', <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>.

<sup>13</sup> According to the Basel Committee on Banking Supervision "many jurisdictions' consent rules also place restrictions on downstreaming data to fourth parties, and on reselling customer data for purposes beyond the customer's initial consent." BCBS, 'Report on open banking and application programming interfaces', <https://www.bis.org/bcbs/publ/d486.pdf>.

**15. What are your views on possible areas to consider for a sound open insurance framework highlighted by EIOPA in chapter 6? Are there additional underlying aspects or other aspects under concrete areas to consider for a sound open insurance framework?**

No comment.

**16. What are the key differences of between banking and insurance industry which are important to consider in light of open insurance implementation? (e.g. higher variety of products, more data, including sensitive health data in insurance).**

No comment.

**17. What are the 'lessons learned' from open banking that might be relevant to consider in open insurance?**

See our responses to Questions 20 and 27.

**18. Do you think open insurance will develop without any regulatory intervention? (e.g. without PSD2 type of compulsory data sharing provisions)**

- Yes
- **No**
- I don't know

See our response to Question 19.

**19. Do you think open insurance should be driven voluntarily by industry/private initiatives or driven by regulatory intervention?**

- Driven by private initiatives
- **Driven by regulation**
- A mix of the two options above

Self-regulatory approaches or industry-wide initiatives to data sharing will not lead to the development of a sound Open Insurance framework. Open Finance cannot develop on its own in a way that promotes consumer choice and competition, while ensuring sufficient security and protection for consumers. Under a voluntary initiative, insurance firms may not have any incentives to engage in data sharing initiatives (for instance, large insurance firms would be discouraged because they fear losing market share to new competitors, small firms because of the investment costs associated with data sharing). Experiences from other markets show that only a clear legal right (based on the explicit consent of the consumers and combined with strong consumer protections) will ensure that consumers are willing and able to easily share their data with third parties.

For instance, in the United Kingdom, prior to the adoption of its Open Banking framework under PSD2, the UK government launched a 'Midata initiative' in 2011 with the aim of giving consumers more access to their personal data held by banking providers in a portable, electronic format. The Midata initiative for current accounts allowed consumers to download their transaction data and upload it to price comparison websites. The standards for the Midata initiative were developed by UK industry, without consulting the needs of consumers and/or third party providers. A 2015 review by the UK's Competition and Markets Authority and evidence from Which?

revealed significant shortcomings with the Midata initiative, meaning that the initiative did not take off and was generally not used by consumers. For Which?<sup>14</sup>, the failure of the Midata initiative in the UK demonstrate the clear limits of a voluntary approach and the need for consumers to be given a clear legal right to access their data based on adequate consumer protections for Open Finance initiatives to succeed.

**20. Do you have views on how the EU insurance market may develop if some but not all firms (e.g. based on different industry-wide initiatives) open up their data to third parties?**

See our response to question 19.

**21. What datasets should be definitely included in the scope of a potential open insurance framework? What data should be definitely excluded from the scope of open insurance framework? Are there any data sets you currently do not have access or do not have real-time access or where you have faced practical problems, but you consider this access could be beneficial? This could include both personal and non-personal data (e.g. IoT devices data, whether data, sustainability-related data, data on cyber incidents etc.). Please explain your response providing granular examples of datasets.**

Under any future Open Insurance initiative, priority should be given to (i) financial data and (ii) non-financial data that is strictly necessary to facilitate the provision of the insurance service. The principle enshrined in GDPR on data minimisation should be fully applied. Any eventual Open Insurance initiative should prioritise facilitating the sharing of data related to (i) product information (policy features, fees or charges, exclusions, etc.) (ii) basic consumer data (such as their name, address, and potentially claims history data).

When defining the exact scope and the requirements for which type of financial and non-financial information could be shared between financial services providers, particular attention should be paid to the potential risks related to the exposure of sensitive information or specially protected categories personal data. Certain categories of personal information should be excluded from the scope of data sharing initiatives under any future Open Insurance framework. For instance, we would question the value of requiring BigTech firms to share sensitive personal information about consumers with insurance firms (such as internet searches, social media data, past shopping habits, etc). Insurance firms are expected to rely on ever-increasing sources of data when pricing and carrying out risk assessment for insurance contracts, and this could lead to more granular pricing and concerns about financial exclusion. Firms also often rely on irrelevant data when pricing insurance contracts (see also our [position paper](#) on Big Data and AI), and further restrictions on what types data parameters can be considered about consumers when pricing insurance contracts or carrying out risk assessments should be considered.

**22. In your opinion, which regulatory/licensing approach would be best for the development of sound open insurance framework (e.g. unlocking the benefits and mitigating possible risks)? Could an increased data sharing require revisions in the regulatory framework related to insurance data? Please explain your response.**

- Compulsory data sharing inside the regulated insurance industry
- **Compulsory data sharing inside the regulated insurance industry and with third parties with bespoke licensing approach**

---

<sup>14</sup> For more information about Midata initiative, see Which's [position paper](#) on 'The pensions dashboard: How can we make sure it works for consumers', pages 32 to 33.

- Compulsory data sharing in certain lines of businesses and/or amongst certain products
- Compulsory data sharing covering only IoT data / sensor data
- Self-regulatory approach to data sharing (no regulatory intervention in addition to the GDPR data portability rules)
- A mix of the approaches
- Other

Self-regulatory approaches to data sharing will not lead to the development of a sound Open Insurance framework. Any eventual Open Insurance framework should be based on compulsory data sharing (based on the explicit informed consent of the consumer) to firms inside the regulated insurance industry and with other authorised third parties, based on a bespoke licensing approach. All firms wishing to access data through Open Finance initiatives should be strictly accredited and supervised by their national competent authorities, including in close cooperation with national data protection authorities. This should ensure that only reputable firms can offer Open Finance related services to clients. It will be also necessary to establish a public register of all accredited data intermediaries, thus easily allowing the consumer to check if the entity is authorised or not.

**23. Could you provide information which helps to evaluate the cost of possible compulsory data sharing framework (e.g. based on your experience on PSD2 adoption)?**

No comment.

**24. In the absence of any compulsory data sharing framework in insurance as it is currently the situation, how do you see the role of EIOPA and national supervisors to guarantee proper market oversight and consumer protection?**

No comment.

**25. This Discussion Paper highlighted some of the ethical issues relevant to open insurance (e.g. price optimisation practices, financial exclusion, discrimination). Do you see additional ethical issues relevant in light of open insurance?**

We agree with the risks identified by EIOPA (see our [position paper](#) on ethical issues related to Big Data and AI for further information).

**26. What functions and common standards are needed to support open insurance and how should they be developed? Please consider this both from self-regulatory angle and from possible compulsory data sharing angle.**

We agree that common standards will need to be developed to support the development of Open Finance initiatives. Common standards should be developed by public authorities in consultation with industry and consumer representatives.

**27. What existing API/data sharing standards in insurance/finance in the EU or beyond could be taken as a starting point/example for developing common data sharing standards in insurance?**

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. Account access to consumer information should be done through dedicated Application Programming Interface (API) standards in order to ensure that consumers' data is shared in a controlled way.

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 (for instance, for accessing information on savings accounts), they employ so-called 'screen scraping' techniques to access consumer data. Screen scraping techniques allow Third Party Providers (TPPs) to access consumers financial transaction data by logging into digital portals on behalf of the consumers using their login and password details. Screen-scraping raises serious security and consumer protection risks<sup>15</sup> that should be addressed in any eventual EU Open Finance framework. Such techniques are unsecure for the consumer, since it requires the sharing of a consumer's personal security credentials (such as their PIN information or their password) with third parties. Furthermore, screen-scraping gives third parties full access to the customer's account, including for example, the ability to access sensitive data that has not been fully authorised by the consumer.

Third parties should also 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 or login information) are not shared with any third parties. 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.

In addition, since the entry into force of PSD2, a large variety of different API standards exist across Europe<sup>16</sup>, meaning that third party firms may need to use different API standards to communicate with different banks when accessing the data of consumers. This leads to challenges, such as inefficiencies for third parties wishing to access banking data and the fragmentation of the digital financial ecosystem. A lack of standardised APIs mean that Third Party Providers must integrate themselves with multiple provider APIs, and that data is not shared in a consistent manner. Under any future Open Finance framework, API standards should be developed in a way that promote interoperability, efficiency and usability for all users, as well as granular data filtering principles in order to be able to adhere to data minimisation principles. 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. Standardisation of APIs reduces barriers to entry and supports innovation, as third parties relying on standardised APIs do not have to integrate with a different technology for each firm that they connect to.

Building on the experience with PSD2, APIs should be specified by the regulator and not be left to solely the industry to develop. This would ensure that the API is in line with regulations such as data protection rules as well as fulfils its function to work as an industry-wide pipeline. For PSD2, the industry did not develop APIs that are in line with 'privacy by design and by default' principles. This must not repeat itself when it comes to sensitive insurance-related data.

---

<sup>15</sup> Which?, 'Open banking vs screen scraping, what are my rights?', <https://www.which.co.uk/consumer-rights/advice/open-banking-vs-screen-scraping-what-are-my-rights-aU0EF8H853Rh>.

<sup>16</sup> BEUC, 'PS2 - Secure communication between banks and third party PSPs', [https://www.beuc.eu/publications/beuc-x-2017-054\\_mgo\\_psd2\\_-\\_secure\\_communication\\_between\\_banks\\_and\\_third\\_party\\_psp.pdf](https://www.beuc.eu/publications/beuc-x-2017-054_mgo_psd2_-_secure_communication_between_banks_and_third_party_psp.pdf)

**28. Do you believe that open insurance only covering insurance-related data could create an un-level playing field for incumbent insurance undertakings vis-a-vis other entities such as BigTech firms. Please explain your response.**

An Open Finance framework with data sharing based on the explicit consent of the consumers should empower consumer to access better financial products and more easily switch between financial services providers, including to services offered by new FinTech and BigTech providers. In exchange for establishing such an Open Finance data sharing framework, some banks and financial institutions are calling for 'reciprocal' data access to the non-financial data held by BigTech platforms (such as a consumer's search history, location data, or other personal information held by such platforms). BEUC firmly opposes proposals to require reciprocal data access by financial services firms to the personal (non-financial) data that Big Tech firms hold on consumers.<sup>17</sup>

The data collected by BigTech firms about consumers is often very extensive.<sup>18</sup> Consumers are often pervasively tracked and profiled online by BigTech firms, and often have no way of knowing which entities process their data and how to stop them. Data collection practices by BigTech firms are often out of control, rife with privacy violations<sup>19</sup> and in breach of European law.<sup>20</sup> Consumers are also often not aware of the extent of data that the BigTech firms hold about consumers. We would question the value of using social media data in the risk assessment and pricing processes of insurance firms (we agree with EIOPA that there should be strict limitations on the type of data that is considered by firms, and that inadmissible data should include personal information held by the GAFAs such as internet searches, social media data, past shopping habits, etc.). For more information about the challenges and risks involved with incorporating non-traditional data into credit scoring (which are equally applicable to insurance risk assessment, see this study<sup>21</sup> commissioned by BEUC on 'The Never-Ending European Credit Data Mess' (pages 37-40).

Tackling the potential risk of an unlevel playing field between the GAFAs and financial services providers can best be solved by a better enforcement of data protection rights under the GDPR (notably the requirements on data minimisation and purpose limitation), rather than opening up the possibility to share such information with financial institutions.

**29. How do you see the market will develop in case the data sharing is extended to non-insurance/non-financial data? What are the biggest risks and opportunities?**

There are significant risks for consumers in extending data sharing to non-insurance and non-financial data. The potential risks that we see are as follows (for more information and our full policy recommendations, please consult our [position paper](#) on the use of Big Data and AI in insurances):

---

<sup>17</sup> BEUC, 'Open Finance should not mean an open bar for consumer data', <https://www.beuc.eu/publications/beuc-x-2020-054-open-finance-should-not-mean-open-bar-for-consumer-data.pdf>

<sup>18</sup> Forbrukerrådet, 'Every step you take', <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf>

<sup>19</sup> BEUC, 'Consumer groups across Europe file complaints against Google for breach of GDPR', <https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html>.

<sup>20</sup> Forbrukerrådet, 'Out of control: How consumers are exploited by the online advertising industry', <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>.

<sup>21</sup> Federico Ferretti, 'The Never-ending European credit data mess', [https://www.beuc.eu/publications/beuc-x-2017-111\\_the-never-ending-european-credit-data-mess.pdf](https://www.beuc.eu/publications/beuc-x-2017-111_the-never-ending-european-credit-data-mess.pdf), pages 37-40.

**Personalised pricing:** The increased accessibility of more granular consumer data combined with AI could increase the capacity of firms to charge differential prices to consumers that are similar in terms of risks and cost to serve. Technological advances could enable firms to develop ever-more sophisticated pricing practices, leading to discriminatory pricing practices and unfair outcomes for consumers.

**Financial exclusion:** An increasing reliance by insurance firms on non-insurance and non-financial data has the potential to increase risk segmentation in insurance, allowing insurance firms to more accurately model a consumer's risk profile and charge corresponding premiums. Increased risk segmentation could lead to consumers with a higher risk being unable to obtain insurance or being unable to afford insurance. For instance, in the Netherlands, our member Consumentenbond witnessed large increases in the premiums for certain home insurance contracts as firms began to rely on larger amounts of consumer data when setting premiums.<sup>22</sup>

Any Open Insurance framework should prioritise the sharing of financial data and non-financial data that is strictly necessary to offer the insurance contract to the consumer.

END.

---

<sup>22</sup> Consumentenbond, 'Premies woonhuisverzekeringen stijgen door gebruik Big Data', <https://www.consumentenbond.nl/nieuws/2018/premies-woonhuisverzekeringen-stijgen-door-gebruik-big-data>.





*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.*