PERSONAL DATA USE IN FINANCIAL SERVICES AND THE ROLE OF FINANCIAL EDUCATION

A CONSUMER-CENTRIC ANALYSIS

OECD

Personal Data Use in Financial Services and the Role of Financial Education

A consumer-centric analysis

Please cite this publication as:

OECD (2020), *Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis* www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf.

Foreword

Technological innovations have greatly increased the capacity of financial services providers to capture, store, combine and analyse a wide variety of customer data, such as their financial situation, preferences, habits and physical location.

These trends can bring benefits to consumers, but come with new risks specific to the financial services sector that may require a comprehensive policy response. Positive outcomes include potentially cheaper and more relevant financial products and access to credit for those without any traditional credit record. In parallel, consumers may not be aware of the extent to which their data is being used. For example, consumers may risk marginalisation as a result of opaque and potentially unfair data-mining practices, or find themselves exposed to fraud and cybercrime.

This report reviews the risks and benefits of these technological developments and suggests policy options to protect consumers, combining robust financial and personal data protection and greater consumer awareness and financial education. It was developed as part of the programme of work of the OECD International Network on Financial Education's (INFE) Working Group on Digital Financial Literacy (see Annex A for a list of members).

The report was prepared by Andrea Grifoni, Policy Analyst, OECD Directorate for Financial and Enterprise Affairs.

Table of contents

Foreword **1**

Background **5**

Introduction 5
The components of a policy framework for the use of personal data in the financial services sector 6

1. Personal data and financial services **9**

1.1. What are personal data 9
1.2. What contributes to "big data" in the financial services sector and how it is collected 9
1.3. Increased personal data generation and processing capacity 10
1.4. How various sources of data are used by financial service providers 13
1.5. What are the implications for consumers? 14
1.6. Consumers' attitudes towards privacy and data as a commodity 19

2. Financial education and awareness **22**

The G20/OECD INFE Policy Guidance action checklist: Focus on personal data 24

3. Conclusions **27**

References **28**

Annex A. List of members of the OECD/INFE Working Group on Digital Financial Literacy . **31**

Tables

Table 1. New elements pertaining to personal data in selected building blocks of the G20/OECD INFE Policy Guidance Note 25

Boxes

Box 1. Big data 11
Box 2. The development of blockchain technologies 12
Box 3. Account aggregation tools 14
Box 4. Responsible stewardship of trustworthy Artificial Intelligence 17
Box 5. Digital security incidents in financial services 18
Box 6. The European Union General Data Protection Regulation (GDPR) 21
Box 7. Digital financial literacy initiatives among OECD/INFE members 22

Background

Introduction

Personal data have come to play an increasingly important role in our economies and societies. While new technologies and responsible data uses are yielding great societal and economic benefits, the abundance, granularity and persistence of personal data brings new risks to the privacy of individuals. Personal data are increasingly used in ways that were not anticipated at the time of creation and collection, with citizens not fully aware of how their personal data are captured, stored and used.

These trends have an impact on the financial services sector and on financial services consumers. Technological innovations have greatly improved the capacity of financial services providers to capture, store, combine and analyse a much greater variety of customer data, ranging from their current or previous location to customer behaviours and preferences. This can bring benefits to consumers, but also new risks that are specific to the financial services sector and that might require a dedicated policy response.

Addressing the implications of the use of personal data in the financial services sector goes beyond financial education. It involves a sound financial consumer protection framework that is fit to protect consumers in digital environments, the existence of national data protection agencies or national data protection strategies with effective resources and enforcement powers, and the need to take into account the levels of digital and financial literacy.

This report contributes, from a financial education perspective, to the identification of approaches to foster behaviours that can protect consumers and entrepreneurs from any negative consequences of such developments in the financial sector.

The report first highlights the different components of a policy response; it then defines personal data and presents the technological, economic and societal developments that have led to an exponential increase in personal data generation and in data processing capacity.

The analysis then focuses more specifically on the financial services sector, explaining how financial services providers collect and use consumers' personal data, before moving to analyse the implications this has for consumers. The report describes in particular the risks that can be incurred by consumers, discriminatory decisions based on the use of big data and threats stemming from cybercrime, before presenting the consumer response to these developments, based on evidence collected through global and national surveys that captured their attitudes with respect to use of their personal data.

In light of these developments and the issues they raise, this report describes specific elements related to personal data that can complement the policy checklist in the G20/OECD INFE Policy Guidance Note on Digitalisation and Financial Literacy (OECD, 2018a).

The components of a policy framework for the use of personal data in the financial services sector

Privacy and personal data protection

The OECD has pioneered international work in the field of privacy and personal data protection.[1] In 1980, this led to the Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, revised in 2013 (OECD, 2013). The societal and technological environment for which these Guidelines were devised has, however, gone through structural changes. As highlighted in the 2013 work conducted for the review of the Guidelines and its privacy principles, today's economies present substantial differences in:

- the volume of personal data being collected, used and stored;
- the range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- the value of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- the extent of threats to privacy;
- the number and variety of actors capable of either putting privacy at risk or protecting privacy;
- the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate;
- the global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

Amongst other things, the Principles call for:

- the provision of reasonable means for individuals to exercise their rights;
- the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy.

Financial Consumer Protection

Privacy and data protection in relation to financial services can be seen as part of a broader framework of financial consumer protection. The G20 High-level Principles on Financial Consumer Protection (G20, 2011) address this through Principle 8 "Protection of Consumer Data and Privacy". This Principle states:

"Consumers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties). The mechanisms should also acknowledge the rights of consumers to be informed

[1] Other relevant OECD instruments in this field are the OECD Consumer Policy Guidance on Mobile and Online Payments (OECD, 2014), the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (OECD, 2015c), the OECD Recommendation on Consumer Protection in E-Commerce (OECD, 2016b). These principles, together with relevant practice, have informed the OECD G20 Toolkit for Protecting Digital Consumers (OECD, 2018e).

about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data".

The implementation of this principle often involves the presence of authorities with a legal mandate for the protection of personal data. Increasingly, across jurisdictions, this is done through a privacy and data protection authority (OECD, 2019c). These independent public authorities supervise, through investigative and corrective powers, the application of the data protection law, provide expert advice on data protection issues, and handle complaints.

As part of its ongoing work on financial consumer protection in the digital environment, the G20 OECD Task Force on Financial Consumer Protection is in the process of developing policy guidance on the protection of consumer data and privacy for financial consumers in the form of updated Effective Approaches to support the implementation of Principle 8.

Financial education and awareness

The need to strengthen financial literacy and awareness on issues around personal data has been addressed in the work undertaken by the OECD/INFE and its Working Group on Digital Financial Literacy.

The G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy (OECD, 2018a), transmitted to G20 Leaders in July 2018, calls for the development of specific core competencies on financial literacy that would support consumers in their use of digital financial services.[2] Two areas in particular are relevant in the context of personal data use by financial services providers:

- empowering consumers, including the most vulnerable, to counter new types of exclusion due to the misuse of various data sources, including big data and digital profiling; and
- protecting consumers and small businesses from increased vulnerability to digital crimes such as phishing scams, account hacking and data theft.

[2] See also the G20/OECD INFE Core competencies framework on financial literacy for adults (OECD, 2016a) and for Youth (OECD, 2015a).

1. Personal data and financial services

1.1. What are personal data

Personal data are defined by the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013) as "any information relating to an identified or identifiable individual (data subject)". Any data that are not related to an identified or identifiable individual are therefore "non-personal" data. However, data analytics has made it easier to relate seemingly non-personal data to an identified or identifiable individual, thus blurring the boundaries between non-personal and personal data (OECD, 2015b).

Indeed, the European Union General Data Protection Regulation (GDPR) (European Union, 2016) (see Box 6), defines personal data as "any information that relates to an identified or identifiable living individual" and stresses that "different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data". The EU framework also stresses that personal data that has been de-identified or encrypted but can be used to re-identify a person remains personal data and falls within the scope of the law.

1.2. What contributes to "big data" in the financial services sector and how it is collected

The financial services industry is among the most data intense of today's economies (OECD, 2015b).

From a consumer-centric perspective, the flow of personal data from the consumer to financial services providers can be categorised broadly based on the consumer's awareness (see Table 1).

Table 1. Data collection channel by consumer awareness

Consumer awareness	Data collection channels
Consumer is aware	Data provided by the customer as part of the KYC process Data given by the customer in order to support a specific product purchase Data given by the consumer in order to use a specific service such as data aggregation tools Data collected when consumers are using specific financial products such as payment services
Consumer is not aware	Data collected by the provider during customer interactions Data collected by the provider on publicly available information (social media) Data shared with the provider by a third party such as credit reference bureau

As described in the next section, the amount of information that consumers provide without awareness (or consent) is constantly increasing, because of technological developments that are pervasive to every aspect of our societies and that determine the creation and the capacity to analyse growing amounts of personal data.

However, it is important to note that even the information that is provided with consumer awareness contributes to the pool of data that is created about consumers: the digitalisation of consumer interactions with financial services providers allows them to capture and indefinitely store information about exchanges between customer and provider, their nature, duration and content. Even a phone call to a customer's bank manager contributes to the pool of customer data.

1.3. Increased personal data generation and processing capacity

1.3.1. The generation of new personal data

Almost universal access to mobile broadband and smartphones, but with regional and socio-economic differences

The last decade witnessed a steady and significant increase in the number of internet users. The developments in mobile technology have also increased the possibilities of accessing the network "on the go" as well as at home. Internet is used more and more by citizens to conduct their daily lives, make economic transactions of any kind, and interact with public authorities. This creates new personal data, which can – to varying extents – be collected and analysed by third parties.

In 2005, around 56% of the adult population in OECD economies accessed the Internet, and 30% used it daily. In 2016, these percentages rose to 83% and 73%, respectively (OECD, 2017a). Across mature and emerging economies alike, mobile subscribers followed the same upward trends and by 2025 the number of unique mobile subscribers isexpected to reach 5.9 billion, which is equivalent to 71% of the world's population (GSMA, 2018).

These general trends do however include differences among countries and sectors of the population. Among OECD countries, in 2016, over 97% of the adult population accessed the Internet in Denmark, Iceland, Japan, Luxembourg and Norway, but 60% or less did so in Mexico and Turkey. There are also differences in usage: in Iceland, Italy, Luxembourg and Norway, the share of daily users is very similar to that of total users, whereas in Mexico and Turkey, many users access the Internet on an infrequent basis (OECD, 2017a).

Differences among user groups are mostly based on age and education, often intertwined with income levels. Uptake by the younger generations is nearly universal, but the picture changes for older customers: over 95% of 16-24 year-olds in OECD countries used the Internet in 2016, compared to less than 63% of 65-74 year-olds. Among older people, education is the major factor affecting internet usage: Internet usage rates for 55-74 year-olds with a tertiary education are generally above or in line with those of the overall population, and in some countries approach the usage rates among 16-24 year-olds.

The Internet of Things

An additional source of consumer data can be traced back to the connected objects and devices that consumers purchase and use. The Internet of Things (IoT) includes all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. While connected objects may require the involvement of devices considered part of the "traditional Internet", this definition excludes laptops, tablets and smartphones already accounted for in current OECD broadband metrics (OECD, 2018c).

This network of Internet-connected objects is able to collect and exchange data using embedded sensors and contribute to the collection of customers' locations and behaviours: telematics insurance systems that capture car drivers' behaviours, smart wearables that can capture health-related information such as distance walked each day or physical activity, and smart homes systems. Globally, the number of connected devices is expected to grow to 50 billion by 2020, up from 9 billion in 2013 (OECD, 2017a).

Consumers might not be able to select what they share through an IoT device; the device will constantly capture and transfer information, in an unobtrusive way and in the background (OECD, 2018d). This creates new risks for consumers. As more and more devices become "smart" (i.e. connected), individuals might lose the capacity to understand the amount of data shared and its privacy implications, let alone monitor its flow and exert some level of control over it. Moreover, consumers are unlikely to have full awareness of what is done with the data collected (Rosner and Kenneally, 2018). In addition, IoT data might be more easily hacked.

Biometrics

An additional source of personal data is biometric data. Biometric data mostly comes from identity authentication through uniquely physical or behavioural characteristics (e.g. facial recognition, fingerprints, voice recognition). This data had never been generated before, or if it had such (as fingerprints), it had not been digitised. This means it can therefore exist without a clear policy framework.

Biometrics carry yet another risk. Unlike passwords that can be changed after hacking, biometric authentication is not so easy to alter.

Box 1. Big data

Economic and social activities have already migrated or are increasingly migrating to the Internet. This takes place while the cost of data collection, storage and processing continues to decline dramatically. In addition, new sources of data are emerging and ever-larger volumes of it will be generated from the Internet of Things, smart devices, and autonomous machine-to-machine communications.

The generation of these huge amounts of data, at levels that are unprecedented in human history, is often referred to as "big data". The OECD defines big data as follows:

> *Big data relates to the huge amount of data generated from activities that are carried out electronically and from machine-to-machine communications (e.g. data produced from social media activities, from production processes, etc.).*
>
> *Big data have characteristics summarised as "3V" (volume, variety and velocity):*
>
> - *volume, referring to vast amounts of data generated over time;*
> - *variety, referring to the different formats of complex data, either structured or unstructured (e.g. text, video, images, voice, documents, sensor data, activity logs, click streams, co-ordinates, etc.);*
> - *and velocity, referring to the high speed at which data are generated, become available and change over time (OECD, 2015b).*

This is in contrast to data processing focusing on low-variety, (relatively) small scale and static datasets, such as customer satisfaction surveys.

1.3.2. Advances in data analytics

These large volumes of data would bear no economic or social value – and no consequences for financial services consumers – if they were not matched by increasing analytical capacities.

Predictive analytics refers broadly to the technologies and procedures followed to process great volumes of data to reveal patterns or correlations, to unlock income-generating insights, and importantly, to predict future events in a more accurate and timely manner.

Advances are most notable, and have the most important consequences in the financial services industry, in the following areas (OECD, 2015a):

- *Data mining*: the set of techniques used to extract information patterns from data sets.
- *Profiling:* the use of data analytics for the construction of profiles and the classification of individual consumers in specific profiles. Credit scoring, price discrimination and targeted advertisements are typical examples of activities involving profiling.
- *Machine or statistical learning* is a subfield in computer science, and more specifically in artificial intelligence. It is concerned with the design, development and use of algorithms[3] that allow computers to "learn" – that is, to perform certain tasks while improving performance with every empirical data set they analyse. Machine learning involves activities such as pattern classification, cluster analysis, and regression.

These advances allow financial services providers to infer sensitive information from data that is unrelated to the financial services profile of an individual, such as past individual purchasing behaviour, electricity consumption, or the activities of circles of contacts on social media.

Box 2. The development of blockchain technologies*

A further development that should be taken into account by financial education policy makers looking into issues relating to the use of personal data is blockchain, despite this not being strictly-speaking a development generating personal data per se, but rather storing it.

Blockchain is a technology with huge potential across a wide range of applications. It utilises distributed ledger technology (DLT) to store information verified by cryptography, which is agreed through a pre-defined network protocol, often without the control of a central authority. The technology can be used to secure the transfer and traceability of value as well as the transfer of data. Its distributed nature of nodes makes it attractive for cyber-security and privacy.

The key point to note with respect to this technology is that the personal information that is stored on the blockchain, because of its decentralised character with immutable blocks, cannot be deleted as these are designed to last forever.

* For more information on technological and policy developments linked to blockchain, please see: www.oecd.org/daf/blockchain/.

[3] An algorithm can be described as "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as an output. An algorithm is thus a sequence of computational steps that transforms the input into the output" (Cormen et al, 2009).

1.4. How various sources of data are used by financial service providers

The increasing wealth of consumers' personal data, and the possibility to analyse it through more and more sophisticated tools and artificial intelligence, can be used by financial services providers - depending on the regulatory framework - in the following functions and services in particular:

- Customer profiling: data stemming from on-line behaviour, geolocation tools, electronic payments and wearables can provide financial service providers with valuable insights on the financial lives of their customers and deliver more detailed customer segmentation.
- Risk assessment: data contributes to an assessment of risks based on multiple sources.
    - Credit: in jurisdictions with positive credit scoring systems (i.e. in which not only negative credit marks are reported by a central authority), big data and augmented analytics determined the emergence of credit scoring tools that integrate thousands of data points about individuals.
    - Insurance: providers could use data aggregation for risk assessment in many different fields, to achieve more precise risk segmentation and risk-based pricing. For example, data generated by activity sensors or physical activity tracker on a mobile phone can be used to determine a policyholder's potential life expectancy. Data analytics can also be applied to telematics data that monitor the behaviour of policyholders and used to mitigate risk in advance based, for example, on location. This can be applied to a range of insurance products, such as health insurance (where consumer's behaviour is tracked and rewarded through wearable devices and/or home connected sensors), car insurance ("Pay as you drive" and telematics), or home insurance (OECD, 2017b).

      Face recognition technology and longevity data can be used for underwriting the provision of life insurance. Face recognition technology is used to predict factors such as chronological age, gender, smoking habits and body mass index (BMI) (OECD, 2017b).
- Robo-advice applied to develop a personal financial plan with a view to saving, saving for retirement, or investing. Consumer data is processed by robo-advice platforms to understand clients' needs and assess risk tolerance, as well as monitoring and adjusting the financial plan (OECD, 2017c).
- Fraud detection, thanks to the near-time (i.e. almost instantaneous) monitoring allowed by artificial intelligence (AI) and, in particular machine learning, which permits a continuous analysis of spending and account management patterns.
- Account aggregation, i.e. the compilation of information from different accounts (checking, investments, savings accounts) in one single place to facilitate personal financial management (see Box 3).

Box 3. Account aggregation tools

Account aggregation tools, which allow consumers to access their accounts (banking, savings, investments, etc.) in one single place, through a website or a mobile app, can function through two mechanisms:

- Screen scraping, through which the customers provides to a third party their login details, passwords and additional security information such as personal questions, which the third party can use to log in as the customer.
- Open banking, as in the European Union (European Union, 2015). This does not require customers to provide passwords to third parties to access accounts on their behalf, and passwords are not shared. Third parties, who are authorised by the financial services authority, connect directly with the customers' banks, through standardised applied programming interfaces (APIs).

Open banking can deliver enhanced capabilities to the marketplace and allow consumers to access all their accounts (banking, savings, investments, etc.) in one single place, through a website or a mobile app. This can contribute to the emergence of improved and innovative products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services, with new entrants in the market and with incumbents innovating as a response.

The key aspect to consider from a financial education perspective is consumer consent* and authorisation, and issues around consumer control. Any provider wishing to access the financial information of a consumer's account must ask for an authorisation, which can focus just on the retrieval of information, or can go further and authorise payment services for example.

Consumers should not feel coerced into granting access to sensitive personal information, such as past bank statements, unless they are aware of this and understand the implications. They should also be aware that, with different modalities according to the applicable regulations, they have the right to revoke authorisation to access, use, or store data.

* See for example the regulatory framework introduced by the Reserve Bank of India for Account Aggregators in September 2016 (RBI, 2016) that, inter alia, includes provisions for customers' explicit consent, and the guarantee of the protection of customers' rights, data security and customer grievance redressal mechanism.

1.5. What are the implications for consumers?

The implications of the increased use of personal data in financial services can be positive for consumers, if they take place within a sound financial consumer protection framework and are matched by sufficient financial literacy and awareness. The increased use of personal data does however also create new risks, which call for an integrated policy response spanning financial education and awareness and financial consumer protection.[4]

[4] For a discussion of privacy and security risks incurred by consumers in the digital environment, see also the Consumer Policy Guidance on Mobile and Online Payments (OECD, 2014).

1.5.1. Cheaper, tailored products with extended reach

The advantages brought to consumers by the digitalisation of finance and by the increasing use that can be made of personal data were presented in the G20 OECD/INFE Policy Guidance Note on Digitalisation and Financial Literacy. Among these, those that are more influenced by the increased availability of personal data and enhanced data analytics tools are:

- Providing access to consumers that are currently excluded from some financial services, for example thanks to the use of big data that can build on non-financial data points to define an alternative credit rating system for those without a credit history.
- Offering more convenient, faster, secure and timely transactions.
- Broadening the range of providers, with new FinTech firms entering the market.

This has already brought benefits for consumers:

- Lower costs, through increased competition and the emergence of FinTech companies in particular in the payments and lending segments.
- Aggregator services that use financial and payment data from bank accounts of consumers for dashboard and accounting products.
- Robo-advice, which has made financial advice available to consumers that could not afford to receive financial advice through human interaction (OECD, 2017c).
- The possibility of creating personalised, built-in nudges in the personal financial management tools used by consumers.

However, the increased availability of personal data and augmented processing capacity also gives financial service providers (whether traditional ones or FinTech) the ability to send targeted offers, which can make it more difficult for consumers, especially those with low levels of financial literacy and awareness, to compare products.

1.5.2. Use of big data and machine learning to inform credit or insurance decisions

Depending on the applicable regulatory framework in each jurisdiction, big data and machine learning can be used to inform or determine the risk profile of consumers, notably in the field of credit and insurance.

While it is not new to analyse personal data to determine clients' risk profiles, this can now be done through a range of data points collected about the individual consumer of which the consumer might not be fully aware. Depending on the algorithm, this can also take place by inferring information on the consumer based on consumers in similar data sets.

Analysis methods increasingly link different datasets and pieces of information from different sources in a way that was not possible before. This blurs the distinction between personal and other data, and makes non-personal data increasingly traceable to individuals, expanding the analytical possibilities of financial services providers (OECD, 2019b).

In the insurance sector, the segmentation of risks and the increased effectiveness of risk-selections can allow insurers to pre-determine which policyholders are likely to bring losses. On this basis, some customers might be offered excellent rates, while others can be excluded from the provision of insurance services.

In the credit sector, the use of alternative data can have important consequences on credit scoring ratings. Traditional credit information, obtained from credit card usage and payments history, can be combined with data points obtained from consumers' online and offline activities. Most of this data does not necessarily have a direct link to individuals' creditworthiness: where consumers shop, what they buy, their social media networks and the activities of their social contacts and/or of people in similar digital networks. Credit providers in the United States have reported a rise of 15% in the accuracy of predictions on consumers.[5]

Research conducted on the creditworthiness of online customers of a German e-commerce company (Berg et al., 2018) shows the superior discriminatory power of a model using both the credit bureau score and the digital footprint variables.[6] This suggests that a lender that uses information from both sources can make more profitable but also more exclusionary lending decisions.

However, recent research also identifies possible additional discriminatory effects deriving from the use of big data, such as exclusion by association in which consumers' social, familial or religious associations have an effect on their credit score (Hurley and Adebayo, 2017). Moreover, the ways in which non-traditional data are used and analysed, which might not be regulated in some jurisdictions, might not be transparent to consumers (and to regulators) as this is based on proprietary analytical tools. This might be done without the accuracy, use limitation, access and dispute protections applicable for example to credit bureaux. In these cases, consumers do not have the ability to challenge what might be an unfair decision, and cannot understand which steps to take to build a better credit score.

[5] "Equifax and SAS leverage AI and deep learning to improve consumer access to credit", Forbes, 20 February, https://www.forbes.com/sites/gilpress/2017/02/20/equifaxand-sas-leverage-ai-and-deep-learning-to-improve-consumer-access-tocredit/2/#2ea15ddd7f69.

[6] The variables taken into account by the study focus only on the interactions with that company, and are: the device type (tablet or mobile); the operating system (iOS or Android); the channel through which a customer comes to the website (such as search engine or price comparison website); a do not track dummy equal to one if a customer uses settings that do not allow tracking device, operating system and channel information; the time of day of the purchase (for example, morning, afternoon, evening, or night); the email service provider (for example, gmail or yahoo); two pieces of information about the email address chosen by the user (includes first and/or last name and includes a number); a lower case dummy if a user consistently uses lower case when writing; and a dummy for a typing error when entering the email address.

Box 4. Responsible stewardship of trustworthy Artificial Intelligence

In September 2018 the OECD set up a 50+ member expert group on AI to develop a set of principles, with representatives of 20 governments and leaders from the business, labour, civil society, academic and scientific communities.

The rationale behind the creation of this group and of subsequent work is the recognition that AI has pervasive, far-reaching and global implications that are transforming societies and sectors of the economy. These implications have the potential to improve welfare and well-being, but may also have disparate effects in our societies and economies, notably regarding economic shifts, competition, transitions in the labour market, inequalities, and implications for democracy and human rights, privacy and data protection, and digital security.

The efforts of OECD governments in this domain resulted in the approval in June 2019 of the OECD Council Recommendation on Artificial Intelligence (OECD, 2019a), which includes the OECD Principles on AI. OECD members plus Argentina, Brazil, Colombia, Costa Rica, Peru and Romania are adherent to the AI Principles.

Two of the Principles are particularly relevant in the field of personal data and financial services:

Human-centred values and fairness

- *AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.*
- *To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art.*

Transparency and explainability

AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

- *to foster a general understanding of AI systems,*
- *to make stakeholders aware of their interactions with AI systems, including in the workplace,*
- *to enable those affected by an AI system to understand the outcome, and*
- *to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.*

The Recommendation also calls on governments to "work closely with stakeholders to prepare for the transformation of the world of work and of society. They should empower people to effectively use and interact with AI systems across the breadth of applications, including by equipping them with the necessary skills".

Source: OECD (2019a), Recommendation of the Council on Artificial Intelligence, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

1.5.3. Rising digital security risks

The digitalisation of our economies and of finance is enriching the wealth of data stored by financial institutions, and offering new ways of accessing them. Financial institutions, because of the potential value of the information stored in their IT systems, are a profitable target for cyber criminals (see Box 5). Data intensity (measured as the average volume of data stored per organisation) is highest in the financial services sector (including securities and investment services and banking) (OECD, 2015b).

In the United Kingdom alone, data breaches reported by financial services firms to the Financial Conduct Authority (FCA) increased by 480% in 2018, to 145 up from just 25 in 2017[7].

Box 5. Digital security incidents in financial services

Digital security incidents affecting the integrity, availability and confidentiality of data stored by financial services providers have become more and more common, and are on the rise globally. Below is a non-exhaustive list of some of the major digital security incidents affecting financial services firm in recent years:

- In 2014, the data of 20 million individuals – 40% of the Korean population – were stolen from three Korean credit card companies[1] (KB Kookmin Bank, Lotte Card and Nonghyup Bank). Personal data included identification numbers, addresses and credit card numbers.
- In 2014 JP Morgan Chase, the largest retail bank in the United States, was the victim of a hack that compromised the data of more than half of all US households – 76 million – plus 7 million small businesses.[2] The data included contact information – names, addresses, phone numbers and email addresses – as well as internal information about the users.
- In 2016 Tesco Bank was victim of a cyber-attack affecting 8.261 out of 131.000 Tesco Bank personal current accounts.[3] Although Tesco Bank's controls stopped almost 80% of the unauthorised transactions, personal current account holders received text messages that were likely to cause customers distress in the early hours of the morning. Some customers suffered embarrassment and inconvenience when they were unable to make payments using their debit cards.
- In 2017, hackers stole the personal data of nearly 150 million people from the databases of Equifax, a consumer credit reporting agency.[4]

1. www.economist.com/finance-and-economics/2014/01/25/card-sharps
2. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/
3. www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf
4. www.gao.gov/assets/700/694158.pdf

[7] https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/

1.6. Consumers' attitudes towards privacy and data as a commodity

The response of consumers to these developments and to the opportunities and risks offered by big data is mixed: if on the one hand, a majority of consumers are aware of threats to their privacy, on the other hand they are also willing to share additional personal information in exchange for better and cheaper services. However, recent research suggests that when consumers consent to share their data to providers they lack an understanding of terms and conditions, including the privacy statement.

1.6.1. Data privacy concerns and awareness of digital security risks[8]

Evidence suggests that consumers value their privacy and are aware of how this can be compromised in today's technological environment. They have concerns about how their personal data can be unlawfully accessed and used, and are aware of the risks posed by cybercrime (access to their accounts, misuse of their personal information).

Consumers are aware of the increasing risks to the integrity of their personal data and their privacy. A 2018 CIGI-Ipsos Global Survey on Internet Security and Trust[9] shows that over half of internet users surveyed globally were more concerned about their online privacy than they were the previous year. In a special 2014 Eurobarometer survey on digital security, online consumers in the European Union reported their top two concerns to be the misuse of personal data and the security of online payments (EC, 2015). National surveys confirm these trends: in the United Kingdom, for example, 42% of those surveyed think it is likely that they will be a victim of cybercrime in the next two years (Ipsos MORI, 2019).

Indeed concerns over data security (data leaks, hacking, etc.) are the second most important reason that would push a consumer to leave their current provider, according to a recent global study conducted by the private sector on the behaviour and preferences of financial services consumers (Accenture, 2019).

Despite these concerns, not all consumers apply the necessary steps to safeguard their personal data online. In the United Kingdom, for example, almost half do not always use a strong, separate password for their main email account. In addition, only 15% say they know a great deal about how to protect themselves from harmful activity, with around 33% stating they rely to some extent on friends and family for help on cyber security (Ipsos MORI, 2019).

Differences in risk perception and in response by target audience

For financial education policy makers, it is important to note that there are differences in perception of online security risks. A recent survey conducted in the United Kingdom (Ipsos MORI, 2019) indicates that 37% of surveyed consumers agree with the statement "losing money or personal details over the internet is unavoidable these days". Those who strongly agree with the statement are more likely to be above 65 years old or have no formal qualifications.

Differences by target audiences are also worth noting with respect to the strategies adopted by consumers to minimise the likelihood of being victim of cybercrime. Indeed, if consumers are concerned about their privacy, not all of them take actions to protect it.

[8] For additional information on digital security and privacy, please see www.oecd.org/going-digital/topics/digital-security-and-privacy/

[9] https://www.cigionline.org/internet-survey-2018

Surveys conducted in the Unites States (Pingitore et al., 2017) and the United Kingdom (Ipsos MORI, 2019) indicate that younger consumers take more proactive actions to safeguard their online privacy, such as adjusting privacy settings on their mobile phones or social media.

1.6.2. Trading personal data for additional benefits

Evidence suggests that consumers are also willing to share additional personal data with financial providers if this results in perceived benefits. Two global surveys conducted by the private sector shed some light on this trend.

The first one addresses data sharing in general and is not focused just on financial services (GfK, 2017). It finds that more than a quarter (27%) of internet users across 17 countries strongly agree that they are willing to share their personal data in exchange for benefits or rewards, such as lower costs or personalised services. The percentage of users who are firmly unwilling to share their data is around 19%. The survey also indicates that Internet users aged 30-40 are most likely to share data for rewards.

A second survey focuses in particular on the financial services sector (Accenture, 2019). This indicates that around 60% of the consumers surveyed globally indicate that they would share more data with banks, insurers, or investment advisory firms if this translated into priority services, pricing benefits, more personalised products or non-regulated financial advice. This percentage increases among categories of consumers that are younger and more digitally keen. These consumers are open to begin making financial transactions through GAFAs (Google LLC, Apple, Inc., Facebook, Inc. and Amazon.com). For these consumers, and for the generations born after the 1990s in particular, GAFAs are also attractive alternatives to traditional financial providers, with 40% of them that would consider banking with Facebook, Google or Amazon. This is even higher in markets such as the United States, where 50% would be willing to make this switch (Accenture, 2019).

1.6.3. Consent is not informed

These shifts are taking place despite consumers not fully understanding the value of their personal data. Research conducted in the United Kingdom (Financial Services Consumer Panel, 2018) to assess how willing consumers are to share their data with third parties in the framework of open banking confirms that consumer consent is not well informed. More than three quarters of consumers (even among those with higher socio-economic and educational background) state that they do not feel informed when they read terms and conditions. In addition, most consumers who give consent to the treatment of their personal data by third-party providers do not understand some of the terms and conditions they have agreed to and hence indicate that their consent it not informed.

Finally, the degree to which they can exercise control over the use of their data is not clear to them – no more than their rights over their data. This point in particular is relevant for financial education and awareness policy makers, as recent landmark advances in the regulation of privacy and personal data use aim to give more control and more rights to consumers (see Box 6).

Box 6. The European Union General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and aims to give more control to EU citizens over their personal data, and how that data are accessed, processed and used. The GDPR sets out seven key principles covering personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); accountability.

The GDPR also gives "data subjects", i.e. all natural persons whose personal data are processed by a controller or processor, specific (new) rights. The Regulation codifies the following fundamental data subject rights:

- The right of access.
- The right to rectification.
- The right to erasure or right to be forgotten.
- The right to restriction of processing.
- The right to data portability.
- The right to object.
- The right not to be subject to a decision based solely on automated processing, including profiling, when this bears legal effects or significantly affects him or her.

2. Financial education and awareness

Public policies dealing with the personal data of financial services consumers have so far focused mostly on data protection and financial consumer protection regulation. National strategies for financial education, apart some notable exceptions (see Box 7), have yet to systematically include this element within the content of their programmes.

The development of new core competencies relating to personal data is made even more relevant as recent changes to privacy regulations in some jurisdictions seek to empower consumers and give them specific rights over their data (see Box 6). Consumers should possess the necessary knowledge and skills to understand the use that is made of their personal data and to fully exercise their consumer rights in this domain.

Box 7. Digital financial literacy initiatives among OECD/INFE members

Members of the OECD/INFE have begun to include financial education and awareness on the importance of personal data within their national strategies and initiatives.

Germany

In Germany the Federal Ministry of Justice and Consumer Protection (BMJV), as the competent authority for consumer policy relating to amongst other things the Information society and financial services, published a comprehensive article on the consumers' rights to their data. The article includes a section on the protection of personality by data protection, a section on how an individual consumer can get information on the data collected already about him or her as well as guidance on how to avoid providing unnecessary data and on how to safely use the internet. There is a free download available with information tailored to elderly consumers.[1]

The German Federal Financial Supervisory Authority (BaFin) provides consumers with practical guidance on the use of their personal data when using financial services. In 2019, BaFin gave an online seminar for elderly people on the Second Payment Services Directive (PSD2)[2] explaining the impact of the directive on electronic payment and online Banking and on alternative payment solutions. There was a special focus on data protection issues.

Portugal

Digital financial literacy is among the key goals of the Central Bank of Portugal's Strategic Plan for 2017-2020. This strategic goal addresses in particular the safe use of digital channels. The adoption of safety procedures by customers is encouraged through awareness campaigns on the Bank Customer website (https://clientebancario.bportugal.pt). The website also features a dedicated page, with contents on digital security such as risks associated with digital channels, and the explanation of what Big Data is, as well as its benefits and risks. This information is accessible to consumers through plain language and an intuitive interface, supported by audio-visual tools.

In 2018, the Central Bank of Portugal launched a digital financial education campaign addressed at young people (#toptip) to raise awareness amongst digital natives on the necessary precautions to be adopted when using digital financial services. The first tip "When using the internet, do you have any idea of the risks?" gives hints on how users should protect their equipment and internet connection from risks such as phishing,

pharming, spyware and SIM card swap. The second tip "Do you use your smartphone to access social networks or email? Or home banking? Do you also make payments with your mobile phone?" focuses on the importance of protecting the large amount of confidential and private information that users have on their mobile phones. The third tip "Is social media your second home?" warns about the risk of sharing personal data in social media. The fourth tip "Do you safely buy online?" clarifies the steps that users should follow before, during and after an online purchase. The fifth tip "What if you are a victim of online fraud?" helps users who have been (or suspect they were) victims of online fraud. The campaign was also delivered through the Instagram account of the Central Bank (@bancodeportugalofficial). The Central Bank sent a brochure with these tips was to all secondary schools and regularly conducts financial education sessions in secondary schools which are in high demand.

Spain

Digital financial literacy is among the key goals of the National Financial Education Plan implemented by the Central Bank of Spain and CNMV for 2018-2021. Digitalisation of financial products and services and the consequent need to strengthen digital financial literacy are seen as key areas of action. The Financial Education Plan is in particular aware of the opportunities and challenges presented by the digital delivery of financial education and an effort will be made in the identification and promotion of financial education initiatives in this area. Digital tools, applications and software will be used to improve access to financial education, strengthen the key competences of financial services users and increase skills in the field of management and control of their finances.

With respect to personal data, the Spanish National Strategy website, *Finanzas para Todos* (www.finanzasparatodos.es), includes an entire section related to protecting personal information, with answers to questions such as: "What personal information should I protect?", "What should I do if I receive an email asking me to confirm my personal information?", "What is spyware?" and "What precautions should I take with online banking?". Similarly, a section on safeguarding personal information is included in the Financial Education Programme for Schools, for students 14–18, and addresses the same questions mentioned above. This programme also includes practical classroom activities with the following learning objectives:

1. Understand the importance of safeguarding our personal information to avoid falling victim to financial fraud;
2. Identify the necessary precautions to take with online banking and other Internet activities;
3. Know the importance of reporting the theft or loss of documents and keeping a written record of the report; and
4. Know the precautions to take for online banking and other Internet activities.

1. www.bmjv.de/DE/Verbraucherportal/DigitalesTelekommunikation/Datenschutz/Datenschutz_node.html

2. www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_191017_digitaler_stammtisch_digitalisierung.html

The G20/OECD INFE Policy Guidance action checklist: Focus on personal data

In light of the need to address the use of personal data within financial education programmes, and to encourage positive behaviours on personal data awareness and management, this report suggests specific elements pertaining to personal data in support of the implementation of the G20/OECD INFE Policy Guidance Note on Digital Financial Literacy.

These new elements should be considered as an additional implementation tool for policy makers and programme designers addressing financial education and personal data, and should be read taking into account the regulatory framework and the financial and digital literacy levels in each jurisdiction.

Table 1. New elements pertaining to personal data in selected building blocks of the G20/OECD INFE Policy Guidance Note

Selected building blocks of the G20/OECD INFE Policy Guidance Note	Specific elements pertaining to personal data
1. Develop a national diagnosis	*Supply side* Scan the current landscape to understand: • How financial services providers use consumers' personal data, in the framework of the applicable national legislation. • The presence of specific actionable rights over personal data in financial services, as per financial consumer protection or data protection legislation. *Demand side* Draw on existing data and analysis, or commission research to understand: • Attitudes towards privacy and personal data use • Consumers' understanding of digital footprint • Online security awareness and behaviours • Appetite for data sharing • Awareness of actionable rights over personal data in financial services, as per financial consumer protection or data protection legislation
2. Ensure coordination	Among public authorities: • Coordinate with, or at a minimum consult, the national data protection authority, if existing, or the public authorities with a legal mandate and effective means in the field of privacy and data regulation[10]. With the private and not-for-profit sector: • Public authorities should seek to harness the knowledge of the private sector, and in particular of FinTech actors, to understand new developments in the field of personal data sharing.
3. Support the development of a national core competency framework on digital financial literacy	
3.a Empowering consumers, including the most vulnerable, to counter new types of exclusion due to the misuse of various data sources, including big data, and digital profiling	
• Appropriately manage their digital footprint to the extent possible:	• Consumers should be aware of the analytical possibilities offered by big data, and that any online activity can be used by financial services providers to customise offers and define cost and range of product offer. • In countries with positive credit scoring systems in particular, consumers should understand that credit scoring decisions can be influenced by personal information that is not related to their personal credit history.

[10] For a global list of national data protection authorities, see: https://www.dlapiperdataprotection.com/index.html?t=authority&c=AR&c2=

Selected building blocks of the G20/OECD INFE Policy Guidance Note	Specific elements pertaining to personal data
• Avoid engaging in risky behaviours involving their personal data, and understand the consequences of sharing or disclosing personal identification numbers, account information, or other identifying information such as address, birth date or government-issued numbers whether digitally or through other channels:	• Target groups that display the lowest familiarity with online transactions and lowest levels of digital literacy should be prompted regularly to take effective measures to safeguard their personal data and privacy.
• Assess the kind of information that is requested by (financial) service providers to decide whether it is relevant and understand how it may be stored and used.	• Target groups that are willing to share more personal information with financial services providers in exchange for benefits, notably younger generations and the more technologically savvy, should be aware of the consequences to their privacy and should share non-essential additional information based on informed consent.
• Increase awareness of consumer rights with respect to personal data, and on the applicable regulatory framework, especially if this gives consumers new rights and discretionary control over their personal data.	• In jurisdictions where changes to personal data regulations have assigned new rights to consumers, they should be informed through awareness campaigns. • Inform consumers of the mechanisms behind the decisions made on their financial lives, in particular when these have been taken without human intervention. • When consumers have the legal right to challenge a decision taken by an algorithm, they should be informed and know how to seek recourse.
3.b Protecting consumers and small businesses from increased vulnerability to digital crimes such as phishing scams, account hacking and data theft	
• Increase awareness of the existence of online fraud and of cyber security risks when choosing and using digital financial services,making financial transactions online, and using account aggregation tools (“screen scraping”).	• Consumers - and the most vulnerable target groups in particular - should be alerted to the need of using strong passwords to protect their personal data and financial transactions online and informed about what to do in case of a security breach.
• Increase awareness of the possibilities offered by account aggregation tools, and how to use and stop using such tools safely given that they are providing access to their account information to third parties.	• Consumers understand data sharing revocation terms and when to revoke authorizations to access, use, or store data. • Consumers understand that through screen-scraping, the passwords and login information remains with the third-party provider also when they stop using the service, increasing the likelihood of the password being stolen or misused.

3. Conclusions

In today's economies, the capacity of financial services providers to capture, store, combine, and analyse a wide variety of customer data, such as their financial situation, habits or physical location, has prompted an adaptation of data protection and financial consumer protection frameworks. While this is necessary, public policies should also aim to reinforce awareness among consumers of the implications of the use of their personal data, and foster behaviours that can protect their personal data while helping them to take a proactive stance to data sharing that is consistent with their own preferences. Such a consumer-centric approach also responds to an evolving regulatory context in which individuals are assigned new rights covering their personal data.

The analysis conducted in this report presents the implications of the use of personal data in financial services from a consumer perspective. It covers both the possible advantages and risks, drawing on existing data to describe consumer attitudes to personal data sharing.

Based on this analysis, financial education policy makers are encouraged to take into account issues relating to personal data when gathering evidence to inform their policies and programmes. This would ideally cover both the supply side, i.e. the use that is made of personal data by financial services providers and the applicable regulatory framework, and the demand side, i.e. consumer attitudes to data sharing and their understanding of the value and implications of their personal data.

Authorities in charge of financial education in each jurisdiction are invited to coordinate or consult with the authorities in charge of personal data protection and financial consumer protection to ensure that financial education policies and initiatives benefit from their expertise and are coherent with existing national frameworks on personal data protection. Similar coordination or consultation should also take place with Fintech providers in order to fully understand new developments in personal data sharing.

Finally, the report identifies specific financial literacy competencies that would benefit individuals and entrepreneurs in this domain, providing new elements pertaining to personal data in support of the implementation of the G20/OECD INFE Policy Guidance Note on Digital Financial Literacy. These additions are for consideration by policy makers, and should be read taking into account the financial consumer protection and personal data protection frameworks in each jurisdiction.

The OECD, through its International Network on Financial Education, and through its horizontal project on digitalisation, will continue to monitor policy solutions implemented at the national level, and to engage in a fruitful discussion at the international level to identify good practices. Thanks to its global nature, the OECD/INFE will also foster the necessary cross-border approach to personal data policies.

References

Accenture (2017), Accenture Financial Services 2017 Global Distribution & Marketing Consumer study: financial services report, www.accenture.com/t20170111T041601__w__/us-en/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Financial-Services-Global-Distribution-Marketing-Consumer-Study.pdf

Accenture (2019), Accenture Global Financial Services Consumer Study, https://www.accenture.com/_acnmedia/PDF-95/Accenture-2019-Global-Financial-Services-Consumer-Study.pdf

Berg T., Burg V., Gombović A., Puri M. (2018), On the Rise of FinTechs – Credit Scoring using Digital Footprints, https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf

Cormen T., Leiserson C., Rivest R. and Stein C. (2009), Introduction to Algorithms, Third Edition, MIT Press

European Commission (2015), Special Eurobarometer 423 Cyber Security - Report, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

European Union (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

European Union (2015), Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

EU Financial Services Users Group (2016), Assessment of current and future impact of Big Data on Financial Services, https://ec.europa.eu/info/sites/info/files/file_import/1606-big-data-on-financial-services_en_0.pdf

Financial Services Consumer Panel (2018), Consenting adults? - consumers sharing their financial data, https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf

G20 (2011), G20 High-level Principles on Financial Consumer Protection, http://www.oecd.org/daf/fin/financial-markets/48892010.pdf

GfK (2017), Willingness to share personal data in exchange for benefits or rewards - Global GfK survey, https://www.gfk.com/fileadmin/user_upload/country_one_pager/NL/images/Global-GfK_onderzoek_-_delen_van_persoonlijke_data.pdf

GSMA (2018), The Mobile Economy 2018, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

Hurley M., Adebayo J. (2017), Credit Scoring in the Era of Big Data, 18 Yale J.L. & Tech. Available at: https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5

Ipsos MORI (2019), UK Cyber Survey Key findings – General public, conducted on behalf on behalf of the National Cyber Security Centre and Department for Digital, Culture, Media and Sport (DCMS), https://s3.eu-west-1.amazonaws.com/ncsc-content/files/UK%20Cyber%20Survey%20-%20analysis.pdf

Joint Committee of the European Supervisory Authorities (2016), Discussion Paper on the Use of Big Data by Financial Institutions, https://esas-joint-committee.europa.eu/Publications/Discussion%20Paper/jc-2016-86_discussion_paper_big_data.pdf

OECD (2013), The OECD Privacy Framework www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

OECD (2014), "Consumer Policy Guidance on Mobile and Online Payments", OECD Digital Economy Papers, No. 236, OECD Publishing, Paris, https://doi.org/10.1787/5jz432cl1ns7-en.

OECD (2015a), OECD/INFE Core competencies framework on financial literacy for youth, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Youth.pdf

OECD (2015b), Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264229358-en

OECD (2015c), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

OECD (2016a), G20/OECD INFE Core competencies framework on financial literacy for adults, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Adults.pdf

OECD (2016b), Consumer Protection in E-commerce: OECD Recommendation, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264255258-en.

OECD (2017a), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, https://doi.org/10.1787/9789264276284-en.

OECD (2017b), Technology and innovation in the insurance sector, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf

OECD (2017c), Robo-Advice for Pensions, https://www.oecd.org/finance/Robo-Advice-for-Pensions-2017.pdf

OECD (2018a), G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy, http://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf

OECD (2018b), G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age, https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf

OECD (2018c), "IoT measurement and applications", OECD Digital Economy Papers, No. 271, OECD Publishing, Paris, https://doi.org/10.1787/35209dbf-en

OECD (2018d), "Consumer policy and the smart home", OECD Digital Economy Papers, No. 268, OECD Publishing, Paris, https://doi.org/10.1787/e124c34a-en.

OECD (2018e), G20 Toolkit for Protecting Digital Consumers, https://www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf

OECD (2019a), Recommendation of the Council on Artificial Intelligence, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

OECD (2019b), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en.

OECD (2019c), "Good practice guide on consumer data", OECD Digital Economy Papers, No. 290, OECD Publishing, Paris, https://doi.org/10.1787/e0040128-en.

Pingitore G., Rao V., Cavallaro K., and Dwivedi K. (2017), To share or not to share, Deloitte University Press, https://www2.deloitte.com/content/dam/insights/us/articles/4020_To-share-or-not-to-share/DUP_To-share-or-not-to-share.pdf

Press, G. (2017), "Equifax and SAS leverage AI and deep learning to improve consumer access to credit", Forbes, 20 February, https://www.forbes.com/sites/gilpress/2017/02/20/equifaxand-sas-leverage-ai-and-deep-learning-to-improve-consumer-access-tocredit/2/#2ea15ddd7f69.

Reserve Bank of India (2016), Master Direction- Non-Banking Financial Company - Account Aggregator, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

Rosner G. and Kenneally E. (2018), Clearly Opaque: Privacy Risks of the Internet of Things, https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54

Annex A. List of members of the OECD/INFE Working Group on Digital Financial Literacy

Austria	Martin Taborsky, Central Bank of Austria (Co-leader)
Netherlands	Olaf Simonse, Ministry of Finance (Co-leader)
Australia	Laura Higgins, Australian Securities and Investments Commission
Austria	Elisabeth Ulbrich, Central Bank of Austria
Brazil	João Evangelista de Sousa Filho, Banco do Brasil
Brazil	José Alexandre Cavalcanti Vasco, CVM
Brunei Darussalam	Rina Hayane Sumardi, Autoriti Monetari Brunei Darussalam
Canada	Chris Poole, Financial Consumer Agency of Canada
Chile	Carolina del Río, Financial Markets Commission (formerly SBIF)
Czech Republic	Alex Ivanco, Ministry of Finance
France	Astrid Delacour, Banque de France
India	Gautam Prasad Borah, Reserve Bank of India
India	Girraj Prasad Garg, NISM
Indonesia	Rela Ginting, OJK
Italy	Roberta Nanula, Banca d'Italia
Italy	Nadia Linciano, CONSOB
Korea	Jin Yong Kim, Bank of Korea
Latvia	Dace Jansone, Financial and Capital Market Commission
Luxembourg	Danièle Berna-Ost, Commission de Surveillance du Secteur Financier
Malaysia	Jeremy Lee Eng Huat, Bank Negara Malaysia
Mexico	Pedro Garza López, Banco de México
Mongolia	Myendu Nurgul, Central Bank of Mongolia
Morocco	Imane Benzarouel, Fondation Marocaine pour l'Education Financière
New Zealand	Celestyna Galicki, Commission for Financial Capability
Pakistan	Syed Samir Hasnain, State Bank of Pakistan
Peru	Juan-Carlos Chong, Superintendency of Banking, Insurance and Private Pension Funds
Portugal	Lucía Leitão, Central Bank
Portugal	Lucélia Fernandes, Portuguese Insurance and Pension Funds Supervisory Authority
Republic of North Macedonia	Kristina Pavleska, Coordinating Body of the Regulatory Authorities for Financial Education in Macedonia
Romania	Anton Comanescu, National Bank of Romania
Singapore	Abigail Ng, Monetary Authority of Singapore
South Africa	Lyndwill Clarke, Financial Sector Conduct Authority
Spain	Emilio Ruiz, Banco d'España
Sweden	Thèrese Wieselqvist Ekman, Financinspektionen
Turkey	Nihal Değirmenci, Central Bank of the Republic of Turkey

www.oecd.org/finance