MOKĖJIMŲ TARYBA

Ministry of Finance of the Republic of Lithuania
Bank of Lithuania
Association of Lithuanian Banks
Association of Lithuanian Payment and Electronic Money Institutions
FINTECH Lithuania
Alliance of Lithuanian Consumer Organisation
Lithuanian Small and Medium-Sized Business Council
Association of Lithuanian Chambers of Commerce, Industry and Crafts
Vytautas Magnus University

https://www.lb.lt/lt/mokejimu-taryba
http://finmin.lrv.lt/lt/veiklos-sritys/finansu-rinku-politika/mokejimu-taryba

REPORT

1 July 2020
Vilnius

Development of open banking in Lithuania: Use cases and implementation guidance

Report of the Open Banking Development Task Force of the Payments Council

ISBN 978-609-8204-40-7 (online)

TABLE OF CONTENTS

Abbreviations

OB – open banking

API – application programming interface

ERPB – Euro Retail Payments Board

EC – European Commission

EU – European Union

IT – information technology

PIS – payment initiation service

PSP – payment service provider

PSD2 – Directive 2015/2366 of the European Parliament and of the Council on payment services in the internal market

AIS – account information service

STI – State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania

Task Force – Open Banking Development Task Force of the Payments Council

EXECUTIVE SUMMARY

The concept of open banking emerged together with services regulated by the updated Directive on payment services in the internal market, i.e. the so-called Second Payment Services Directive (PSD2).[1] The scope of PSD2 is indeed limited rigidly defining only the scope of information available and the procedure for initiating payments. That said, PSD2 sets out OB principles that might have a broader application to other financial services and even be expanded to cover other services. OB is based on a model where access to customer data or services of an institution is granted subject to pre-defined conditions to all eligible institutions that are third parties. However, such access may also be granted subject to bilateral agreement.

Following a public consultation, the Lithuanian market participants agreed that the OB topic were to be developed further. The Payments Council decided to deal with the topic and established the Open Banking Development Task Force (hereinafter – the Task Force) bringing together experts of all relevant areas. The Task Force was given the task of establishing OB use cases to be implemented and identifying any barriers to implementing them.

Like across the EU, in Lithuania payment service providers (PSPs) focused on developing application programming interfaces (APIs). APIs provided for in PSD2 were to be completed by 19 September 2019. However, even past that date some PSPs did not yet deliver such APIs while the functioning of the APIs completed was stabilised in real time. As market participants were focused on the development of APIs required by PSD2, there was not much space left to devote any attention to foster innovations.

EU-wide work performed on OB development has so far been suspended. The development of the SEPA API Access Scheme was suspended while work to develop APIs required under PSD2 was ongoing. In the meantime, the European Commission (EC) launched a public consultation on a strategy of digital finances and retail payments also touching upon OB. OB development will also be influenced by economic implications of COVID-19. The implementation of OB use cases is very likely not to be one of the PSP priorities in the immediate future.

For the purposes of this report the scope of OB is limited to financial services including insurance services. The debate however has shown that data exchange interests may be very broad and cover various aspects of personal data. When examining and evaluating OB use possibilities, cases are divided by the nature of service and applicable regulation.

The implementation of OB cases calls for some adaptation of IT systems and coordination between the entity controlling data and providing services and the third party (the intermediary). Invested funds and maintenance costs must be covered, which means that an OB use case must yield benefits. Such benefit sharing between the parties involved in providing OB services is what mostly determines whether an OB use case will be economically sustainable. On the other hand, benefits may arise not only in the form of revenue but also as savings (e.g. in risk management) or benefits to society.

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

One of the key aspects of OB is personal data protection. It requires a lot of attention. Every OB use case calls for an assessment of its impact on personal data protection including data transmission, necessity and proportionality aspects.

An evaluation of the set of OB cases has shown that the biggest development potential lies with solutions aiming at evaluating customer creditworthiness, reducing the risk of fraud, money laundering and terrorist financing, developing financial analysis and management. Recommendations on further work are drawn up based on the above.

1. Obtaining personal (corporate) account information and data on other financial services used in order to, but not limited to, evaluating personal (corporate) credit score.

Recommendations

1.1. To form a dataset which could be used at least in the Baltic States and align it.

1.2. To present the dataset and propose it as a component of the Berlin Group Standard.

2. Enhancing activities relating to fraud risk management and the prevention of money laundering and terrorist financing by giving confirmations or denials on accounts and their holders

Recommendations

2.1. To carry out a legal implementation analysis covering an assessment of impact on personal data protection and to submit proposals on the need to introduce legal amendments.

2.2. If need be, to draft and submit proposals to responsible authorities on introducing legal amendments.

2.3. To develop and install technical interfaces and draft the rules on their use.

3. Dedicated educational and analytical website and mobile app not linked with a specific PSP

Recommendations

3.1. To create and maintain a dedicated website and a mobile app.

3.2. To develop a financial model, and provide for financing sources.

3.3. To prepare a dataset which could allow receiving information on services via the interface.

1. OPEN BANKING CONCEPT AND ITS DEVELOPMENT

1.1. Open banking concept

The provisions of PSD2 entered into force across the EU on 18 January 2018. Among other requirements, the Directive also provides for access to payment accounts that, subject to consent granted by account holders, PSPs would give to licensed third parties such as providers of payment initiation services (PIS) and account information services (AIS). In practice, such access means that account information (balance/statement) is displayed in a digital environment envisaged by the AIS provider (a website or a mobile app) and payment is initiated from own account with the PSP via the digital environment secured by the PIS provider.

Even though the quantity of information held by the AIS provider that is to be disclosed is limited, the Directive does not forbid to disclose more information. However, this would fall outside the scope of PSD2. In such a case the conditions laid down in PSD2 would not be binding and access to information would be regulated by general legal rules and requirements thereof, e.g. legal rules applicable to contractual relations, requirements for personal data protection, etc.

The purpose of granting access to accounts is to enable existing and new market participants to develop new financial services, thus increasing competition in financial and payment sectors as well as improving the performance of these sectors. Speaking broadly, such targeted disclosure reflects the idea of OB.

OB is based on a principle where access to customer data or services of an institution is granted subject to pre-defined conditions to all eligible institutions that are third parties. It may be regulated by legislation or a general market agreement taking the shape of a scheme with self-regulation mechanisms. However, it is often the case that two institutions reach a mutually beneficial agreement that one of them will grant the other access to any customer data or services available. This may also be deemed an OB manifestation.

1.2. Open banking in Lithuania and the EU

The authentication service via a bank has been provided to third parties in Lithuania long ago but it has not been known as OB. This service is still used by both private and public institutions (e.g. the STI, the eGovernment) and this is mostly due to the frequent use of authentication tools provided by banks. Internet banking services are accessed more often than other services, which has promoted certain habits and trust in such tools. Such a service is not however a financial service.

The provision of PIS in Lithuania started even before PSD2 was adopted. It was provided under the conditions of the then effective legal regulation while its interpretation and the diversity of views showed a lack of legal certainty. The technology used to provide PIS (screen scrapping) is controversial, which would render it unsustainable in the long run both as regards security and deployment of IT resources. The implementation of PSD2 became a foundation for tackling legal and technical issues.

The principles of accessing a payment account stipulated in PSD2 and non-uniform scope practices in place in other countries of the world prompted the Bank of Lithuania to consider

the possibilities for developing OB in Lithuania. The Bank of Lithuania carried out an analysis and launched a public consultation seeking to establish market participants' views on OB development and OB prospects. The results of the consultation[2] showed that market participants did support the OB development initiative, new ones being more enthusiastic while the experienced incumbents remaining rather reserved. The Bank of Lithuania therefore decided to bring market participants together for further work on OB development.[3]

The format of the Payments Council was seen as optimal for dealing with practical matters of OB development because that forum comprises representatives of various parties concerned. The Bank of Lithuania proposed this topic to be examined by the Payments Council and received support. A meeting of the Payments Council on 18 April 2019 decided to establish the Open Banking Development Task Force of the Payments Council (hereinafter – the Task Force).

On the EU level the OB development initiative was taken up by the Euro Retail Payments Board (ERPB).[4] It initiated the development of a SEPA API Access Scheme[5] that would cover interfaces of PSPs managing access to accounts that fall outside of the scope of PSD2. The Scheme must set out the organisation of management, the operating model and standardised APIs. In January 2019 the ERPB established a working group to start the work. Still, the preparation by PSPs to implement PSD2 requirements called for much effort and attention, so in summer 2019 the ERPB suspended further work towards to the SEPA API Access Scheme. As of July 2020, the work on the Scheme is still under suspension.

Experience shows that practical preparedness to make a transfer to PIS and AIS throughout EU required more effort than initially estimated. In 2020 many PSPs including those in Lithuania are still working on properly implementing PSD2 and the requirements of related regulatory standards. Many market participants are forced to rethink their operational priorities regarding their expectations of economic and business environment in the aftermath of COVID-19 pandemic. This may also affect OB implementation deadlines.

That said, OB remains on the EU institutional agenda. The EC has included OB development matters in its public consultations on digital finance[6] and a retail payments strategy.[7] This suggests that in the medium term, OB development will remain one of the areas for the development of EU financial services.

2. ANALYSIS OF OPEN BANKING APPLICATIONS IN LITHUANIA

The Task Force has carried out an analysis of OB cases against the objective set by the Payments Council. That objective is to identify the OB use cases of most relevance to the market that fall outside of the scope of PSD2 and to define the needs that would make it possible to implement the selected use cases taking into account the possibilities of financial

[2] Published at https://www.lb.lt/uploads/documents/files/Teisine%20informacija/Konsultacijos/Open-Banking-in-Lithuania.pdf.
[3] See https://www.lb.lt/lt/naujienos/lietuvos-bankas-skatins-atvirosios-bankininkystes-pletra.
[4] The ERPB (Euro Retail Payments Board) is a forum moderated by the European Central Bank where representatives of PSPs and payment service users deal with strategic matters relating to the euro retail payments market.
[5] See https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/Mandate_of_the_working_group_on_a_SEPA_API_access_scheme.pdf.
[6] See https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_en.
[7] See https://ec.europa.eu/info/consultations/finance-2020-retail-payments-strategy_en.

market participants and evaluating EU-wide OB initiatives, applicable requirements and limitations. In a meeting of the Payments Council in 2020 the Task Force is also expected to present its activity report and needs-based recommendations to the parties concerned.

The Task Force has examined OB applications in Lithuania by focusing on individual use cases. Possible use cases have been examined grouping them by the nature of service and applicable rules. Below is a table (see Table 1) summarising the use cases analysed.

Table 1. Overview of OB use cases analysed by the Task Force

<table>
<tr><td rowspan="2"></td><td rowspan="2">Public information</td><td rowspan="2">Covered by PSD2</td><td colspan="2">Not covered by PSD2</td></tr>
<tr><td>Individual user data</td><td>Internal data of the payment service provider managing the account</td></tr>
<tr><td></td><td colspan="4">Account information services</td></tr>
<tr><td>Comparison services</td><td>Service fees
Information on interest rates</td><td colspan="2"></td><td>Non-confidential information on services</td></tr>
<tr><td>Aggregated data</td><td></td><td rowspan="4">Account information</td><td rowspan="2">Financial services used</td><td></td></tr>
<tr><td>Analytical tools</td><td>Analysis based on public information and information provided by the user</td><td>Non-confidential information</td></tr>
<tr><td>Reporting tools</td><td>Service fees, interest rates, etc.</td><td colspan="2"></td></tr>
<tr><td>Information exchange with parties concerned</td><td></td><td>Provision of user information (e.g. place of residence as delivery address for e-commerce)</td><td>Data of accounts used for fraud and confirmed cases of money laundering and terrorist financing</td></tr>
<tr><td>Credit risk assessment</td><td>Access to public sector databases</td><td>Creditworthiness assessment based on account information for its holder</td><td>Creditworthiness assessment for the account holder or third parties based on services used</td><td>Creditworthiness assessment using non-confidential information</td></tr>
<tr><td></td><td colspan="4">Initiation (provision) of services</td></tr>
<tr><td>Payment initiation service</td><td rowspan="6">Not applicable</td><td>Electronic and mobile commerce</td><td>Making deposits</td><td rowspan="6">Not applicable</td></tr>
<tr><td>Customer authentication</td><td></td><td>Authentication for third parties</td></tr>
<tr><td>Information exchange for know-your-customer purposes</td><td></td><td>Provision of information for know-your-customer (KYC) purposes to third parties</td></tr>
<tr><td>Ordering services through an intermediary</td><td></td><td>Ordering automated electronic bill payments through a service provider</td></tr>
<tr><td>Placing orders</td><td></td><td>Securities transfers through an intermediary</td></tr>
<tr><td>Asset management</td><td></td><td>Asset management orders through an intermediary</td></tr>
</table>

OB use cases analysed are divided into two groups: cases where information is used or exchanged and cases where certain services are initiated (provided).

I. OB use cases where information is used or exchanged

1. Comparison services:

(a) service fees;

(b) interest rates.

It may be possible to develop websites where one could compare fees set by various banks (possibly including other service providers, e.g. providing payment services) and interest rates on loans offered. It should be noted that such services are already provided using screen scrapping. For the purposes of providing such services this method is deemed adequate, which is why it will no longer be analysed within the OB development context. That said, the members of the Task Force have agreed that such information provided in an additional API-compatible format would be processed in a more efficient manner;

(c) non-confidential internal information about services provided.

Until it is not clearly defined what information that would be, no specific need to develop this area has been identified. It is however agreed that standardisation and provision of open information in a uniform format would be welcome and would simplify technical implementation should the need for such information arise.

2. Aggregated data and analytical tools:

(a) publicly available data are entered.

Like in the case of comparison services, screen scrapping is used where needed. No separate further analysis is needed for this case because it is included in other use cases of analytical tools;

(b) account information.

This PSD2 requirement is implemented as needed and there is no need to develop the case further;

(c) other financial services are used;

(d) non-financial services.

Relevant data controlled by the state (Sodra and the STI). A larger data volume may be very broad and hard to define. It is limited to financial service data.

3. Reporting to supervisory authorities

There seem to be numerous possibilities for streamlining reporting to supervisory authorities but there is a parallel RegTech initiative[8] aiming at increasing regulatory efficiency when digitalising compliance and reporting processes, so any further analysis of this case would overlap with the work on implementing that initiative and would be meaningless.

4. Information exchange with the parties concerned:

(a) exchanging account and service information.

[8] See https://www.lb.lt/lt/reguliavimo-technologijos-regtech.

It may be useful when assessing customer creditworthiness and considering the provision of leasing and insurance services. It has been decided that in order to assess the development of this area there is a need to consider cooperating with other area within the financial sector. That said, representatives from many sectors have raised the issue of equal conditions when providing or exchanging data. There are some concerns that when granting access and providing service data information may be used against a competitor. Therefore, further prospects for developing such OB use cases are currently not envisaged;

(b) delivery address information when paying on e-commerce sites.

PSPs have been seen to fail to ensure that customer address and other data they have are updated in due time. Moreover, a person may order goods or services to different or provisional addresses and have several phone numbers or email addresses. It has therefore been decided not to develop this case in the OB context;

(c) information exchange on accounts used for fraud with a view to combat fraud cases;

(d) information exchange on accounts and their holders and payment transactions linked with confirmed cases of money laundering or terrorist financing or where there is reasonable suspicion that they may be linked thereto (this would help to combat such crime and efficiently ensure compliance).

There seem to be a need for cooperation in combating fraud and money laundering or terrorist financing ((c) and (d)) bringing high added value. This would however imply exchanging personal data, which has given rise to doubts regarding legal restrictions, especially concerning the enforcement of requirements for personal data protection. In this case it is necessary to assess the impact on personal data protection concerning the necessity of data exchange (its scope and cases), the need-to-know principle (data may only be transmitted to those who need them) and proportionality (only as much data as the other party needs for statutory purposes may be transmitted).

5. Credit risk assessment:

(a) access to public register information.

The members of the Task Force expressed the need and believed it highly beneficial in making internal processes more efficient if it were possible to receive information from national public registers. However, such matters are already dealt with in the KYC Process Optimisation Report[9] approved by the Payments Council, which was why it was decided not to analyse this use case in the OB context any further;

(b) creditworthiness assessment based on account information and provision of creditworthiness information to the account holder;

[9] The report is published at https://www.lb.lt/uploads/documents/files/musu-veikla/mokejimai/Apie-mokejimu-rinka/Mokejimu-taryba/KYC%20proceso%20optimizavimo%20galimybes.pdf.

(c) creditworthiness assessment based on financial services used and provision of creditworthiness information to the service user and/or third parties.

Both (b) and (c) cases do not make full use of creditworthiness assessment possibilities. According to creditworthiness assessors, to assess and forecast a customer's behaviour and to provide professional consultations and solutions meeting the customer's needs to the customer or third parties it is necessary to have access to additional customer information but it is not currently provided because its provision is not envisaged in the Republic of Lithuania Payments Law or such information is listed as optional. Therefore, financial institutions provide no or little such information. The provision of additional information (e.g. the transaction code) would also assure the quality of profiling. Thus, in order to achieve quality assessment or profiling of customer information, apart from the information listed in the Republic of Lithuania Payments Law, the following information would also be needed:

- account holder data;
- company code;
- customer address;
- merchant category code (MCC) or activity code;
- data on financial liabilities;
- deposit or securities account and other account information;
- transaction code.

The need to obtain additional information is valid for assessing the creditworthiness of both natural and legal persons.

It has been decided to consider implementing this OB use case further. The most relevant issues include legal evaluation of profiling and drawing a line between profiling and creditworthiness assessment. It is also necessary to assess the impact on personal data protection and envisage measures necessary for protecting the rights and legitimate interests of the data subject (the user).

It is noted that personal data collected for the purpose of creditworthiness assessment must be compatible not only with the purposes of processing but also with other requirements for personal data protection. For example, if for the purpose of creditworthiness assessment data on the subject's place of residence are collected, this may be seen as a breach of the data minimisation principle because superfluous data on poor residential areas have nothing to do with someone's creditworthiness. Moreover, such profiling of individuals may give rise to adverse legal consequences for data subjects, which may lead to sanctions against undertakings carrying out certain processing actions.

II. OB use cases where services are initiated (provided).

1. Payment initiation service:

   (a) payment initiation through a third party when making a purchase at e-commerce sites (e-shops).

This case falls within the scope of the Republic of Lithuania Payments Law and other legislation regulating the provision of PIS. Technical means are already in place and are adjusted through a regulatory process. Thus, there is no need for additional analysis of this case in the OB context;

(b) placing a deposit through a third party or from another credit institution.

Two options for placing a deposit have been analysed. The first one is where a deposit is placed with a credit institution where the person is a client. There is no need to analyse this option in the OB context as it is implemented in internal systems of the credit institution. The members of the Task Force believe, however, that the second option where a deposit may be placed by a person other than a credit institution customer is to be analysed. The main issue arising when implementing this OB use case would be digital onboarding. Firstly, to develop this case, there is a need to deal with the matter of establishing a business relationship remotely.

2. Customer authentication:

(a) verification of customer identity for a third party.

This OB use case in Lithuania is already in place and in use. However, some consideration has been given to the authentication of customers of foreign institutions and customers of Lithuanian institutions abroad. The most realistic option would be to implement it in the Baltic States where there are institutions belonging to the same group and the authentication tool Smart ID[10] is put to use on a broader basis. Within the EU any changes to customer authentication should be associated with actions expanding the application of the provisions of the eIDAS Regulation.[11]

3. Ordering services through an intermediary:

(a) a service for ordering automated electronic bill payment.

According to the members of the Task Force, the functionality of the electronic bill payment service is sufficient, which is why it has decided not to analyse this use case in the context of OB development any further.

4. Placing orders:

(a) placing securities transfer orders through an intermediary. This would be a service similar to PIS.

5. Asset management.

Placing asset management orders through an intermediary.

This case would also be similar to PIS. That said, the scope of asset management orders is much broader and their nature is more complicated, which is why this case should be analysed separately.

[10] Smart ID may be offered as an electronic identification tool with a certain trust level or as qualified digital signature.
[11] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Both (a) and (b) are currently seen as rather theoretical matters. In Lithuania there are not many users of such services and there are not many customers holding securities either. It is therefore considered that the development of these complex OB use cases would not be economically viable.

3. NEEDS TO DEVELOP OPEN BANKING

The main reason to implement OB use cases falling outside the scope of PSD2 is benefits to be delivered by a use case minus implementation costs. The implementation of all OB cases calls for preparing IT tools and aligning legal instruments. Both access-granting financial institutions and connecting third parties would undertake to implement an OB use case where its benefits exceed its costs and are shared in a balanced manner. Benefits should be continuous for the operating model to be sustainable.

Benefits of implementing OB use cases do not necessarily take the shape of revenues. These may also be new services with societal benefits. For example, when collecting information on accounts and financial and insurance services used and presenting it in a user-friendly way at the same time giving financial management advice, financial education is being developed. Another type of benefits is cost savings or a new efficient solution for managing risks associated with financial services.

In all cases benefits are largely dependent on the scale of service use, i.e. the numbers of operations and users. In this respect the Lithuanian market is small. Therefore, when implementing OB use cases there is a need to consider using them outside of Lithuania, primarily in the Baltic region, where many financial market participants belonging to the same groups are active in three or two countries.

Benefits of every OB use case must be compatible with fundamental human rights, i.e. the right to privacy and the right to personal data protection, at the same time guaranteeing consumer rights. When drawing up a technical specification for every new OB use case, there is a need to assess the impact on personal data protection in advance and to identify measures how the implementation of a specific OB use case would ensure not only access to personal data but also the lawfulness of data processing. These requirements are not in themselves seen as barriers to OB development but there is a need to take additional action to ensure the compatibility of rights.

4. RECOMMENDATIONS ON OPEN BANKING USE CASES

Following an analysis of the set of OB use cases covered and the factors discussed, there is a need to focus on works relating to the following OB use cases.

1. Obtaining personal (corporate) account information and data on other financial services used with a view but not limited to evaluating personal (corporate) creditworthiness

The main need is to identify and align a dataset so that all account managers and service providers providing data would give information suitable for the aligned dataset. Technically

access to information may be assured by employing technology and authentication solutions similar to solutions used in interfaces developed when implementing PSD2 requirements. Where data of the dataset are suitable for use for other purposes as well, subject to the user's consent they may be used for purposes other than creditworthiness assessment. However personal data processing for purposes other than those initially envisaged is only allowed where it is compatible with such new purposes. Personal data collected for the purpose of creditworthiness assessment must be compatible not only with the purposes of processing but also with other requirements for personal data protection. A person's consent for data transmission must be granted in a clear and understandable manner through active actions of the user.

Recommendations

1.1. To make a dataset to be used at least in the Baltic States and align it.

Addressed to: providers of creditworthiness assessment solutions, banks and electronic money institutions. If need be, the Bank of Lithuania might moderate such cooperation.

1.2. To present the dataset and propose it as a component of the Berlin Group Technical Standard.[12]

Addressed to: the Association of Lithuanian Banks.

The expected implementation date is 2021.

2. Enhancing activities relating to fraud risk management and the prevention of money laundering and terrorist financing by giving confirmations or denials on accounts and their holders. This may be a confirmation or denial that the recipient's name and surname match the account number provided as well as a confirmation or denial that an account is suspicious, used for fraudulent purposes or suspected of being used for money laundering, or that the person's name and surname match the name of a person involved in fraud, etc.

The main purpose is to ensure from the legal standpoint that a confirmation or denial of such information is compatible with requirements for personal data protection and to establish what solutions ensure optimal compliance with such requirements. Establishing and managing technical interface requirements. Implementing and maintaining interfaces.

Recommendations

2.1. To carry out a legal implementation analysis covering an assessment of impact on personal data protection and to submit proposals on the need to introduce legal amendments.

Addressed to: banks, the Association of Lithuanian Banks.

2.2. If need be, to draw up and submit proposals to responsible authorities on introducing legal amendments.

Addressed to: the Ministry of Finance of the Republic of Lithuania, the Bank of Lithuania.

[12] Berlin Group is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common scheme- and processor-independent standards. See https://www.berlin-group.org/psd2-access-to-bank-accounts.

2.3. To develop and install technical interfaces and draw up the rules on their use.

Addressed to: banks, electronic money institutions, the Association of Lithuanian Banks.

The expected implementation date is 2022.

3. Dedicated educational and analytical website and mobile app not linked with a specific PSP. Both tools would link financial literacy development materials and AIS and access to other information on a person's financial services. This would bring social benefits. Both tools may be solely educational or also cover personal finances when providing AIS and supplementing information on other financial services of the person. Information would be accessible through an interface with the institution providing the service.

The main purpose is a financial model that would ensure the viability of the service; the tool is offered by an institution entitled to provide AIS; a dataset to be used for obtaining information on financial services through the access interface.

Recommendations

3.1. To create and maintain a dedicated website and a mobile app as described.

Addressed to: banks, other PSPs entitled to provide AIS; the recommendation is to be implemented in cooperation with consumer organisations.

3.2. To develop a financial model and provide for financing sources.

Addressed to: the Association of Lithuanian Banks, FinTech associations, a ministry of the Republic of Lithuania (including the Ministry of Education, Science and Sports).

3.3. To make a dataset making it possible to receive information on services via the interface.

Addressed to: banks, the Bank of Lithuania.

The expected implementation date is 2021.