



Good practices on the implementation of regulatory technical standards

MS approaches on PSD 2 implementation: commonalities in risk management and incident reporting

DECEMBER 2018



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquiries about this paper please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2018
Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-9204-279-0, DOI 10.2824/98934

Executive Summary

The Second Payment Services Directive¹ (PSD2) was adopted by the European Parliament on 25 November 2015. The directive entered into force in January 2016, but Member States had two additional years to transpose the directive into their national legislations.

The main objective of this study is to identify the differences introduced by Member States in the implementation of the PSD2. In particular, the aim is to analyse the adaptation of the PSD2 guidelines in the field of security, such as measures for operational and security risks, and the notification of major incidents.

In addition, an overview will be provided of how different EU Member States approach the transposition of the directive and the preparation of Member States by requiring them to comply adequately, for example, through the competent authorities for registration, authorisation, and supervision of payment service providers (PSPs). PSPs have to ensure the confidentiality, integrity, authenticity, and security of sensitive payment data and personalised security credentials of payment service users. In order to meet these requirements, PSPs must implement the guidelines set out in the directive, regulatory technical standards, and best practice guidelines.

For this reason, ENISA has launched a project to ascertain the real state of the PSD2 implementation in the different Member States. The main purpose of this project is to provide an overview of the transposition of the PSD2 and of how each country is carrying out the implementation.

Transposition of the PSD2 is, at the time of publication, on-going with 23 Member States having completed the transposition and five Member States where the transposition is expected to be completed by the end of 2018. Some of the main observations regarding the transposition in the different Member States are the following:

- As regards the competent national authorities for supervision, monitoring, and reporting of major incidents, Member States have adopted different approaches, some opting for a single entity, while others dividing the tasks among different actors.
- As regards the security measures for operational and security risks, most of the Member States will apply the guideline published by the EBA
- As regards major incidents reporting in Member States, most states directly apply the document published by the EBA
- As regards notification thresholds, most Member States have followed the EBA notification guidelines, though some have introduced minor modifications.

Finally, requirements regarding security measures and incident notification are part of both the PSD2 and the NIS Directive; the report provides a mapping between the relevant requirements as a useful tool for operators that need to comply with both.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>

Glossary

MS	Member State
CA	Competent Authority
EBA	European Banking Authority
ECB	European Central Bank
ENISA	European Union Agency for Network and Information Security
PSP	Payment Service Provider
ASPSP	Account Servicing Payment Service Provider
PIS	Payment Initiation Service
PISP	Payment Initiation Service Provider
AIS	Account Information Service
AISP	Account Information Service Provider
PSU	Payment Service User
SCA	Strong Customer Authentication
DL	Dynamically Link
EEA	European Economic Area

Content

Executive Summary	3
Glossary	4
1. Introduction	7
1.1 Context and objectives of the study	7
1.2 Target Audience	7
1.3 Methodology	8
1.4 Structure of the document	8
1.5 Source of data and information	8
1.6 Scope of the report	9
1.7 Types of actors	9
2. Overview of the implementation of the PSD2	11
2.1 Current Status by Member States	11
3. Good practices on the transposition of PSD2	16
3.1 Overview	16
3.2 Guidelines on the security measures for operational and security risks under PSD 2	17
3.3 Guideline on major incident reporting under PSD 2	19
4. Annex A – Country Details	23
4.1 Austria	23
4.2 Belgium	24
4.3 Bulgaria	25
4.4 Croatia	26
4.5 Cyprus	28
4.6 Czech Republic	29
4.7 Denmark	31
4.8 Estonia	32
4.9 Finland	34
4.10 France	35
4.11 Germany	37
4.12 Greece	39

4.13 Hungary	41
4.14 Ireland	43
4.15 Italy	45
4.16 Latvia	46
4.17 Lithuania	48
4.18 Luxembourg	50
4.19 Malta	51
4.20 Netherlands	53
4.21 Poland	55
4.22 Portugal	57
4.23 Romania	59
4.24 Slovakia	61
4.25 Slovenia	63
4.26 Spain	65
4.27 Sweden	67
4.28 United Kingdom	69

1. Introduction

1.1 Context and objectives of the study

The main goal of the Second Payment Services Directive (PSD2)² is to promote competition and innovation in financial services and to protect the security of payment service users (PSU). It will affect everything, from the way payments are made online, to what information is sent when making a payment. PSD2 focuses on the use of technology in financial services, introducing new technological requirements and measures to guarantee the confidentiality, integrity, availability, and authenticity of user information.

The goal of this study is to:

- Analyse how Articles 95, 96, and 98 of the PSD2 are transposed nationally in all [28 Member States](#) of the European Union (EU);
- Analyse common aspects and differences among the different EU Member States with regard to the transposition of the aforementioned articles of the PSD2; and
- Identify good practices in the implementation of PSD2, taking into account the needs of national authorities, the needs of industry, the [European Central Bank](#), and the [European Banking Authority](#).

1.2 Target Audience

The target audience for this report is the [European Banking Authority](#) (EBA), the [European Central Bank](#) (ECB) and the national competent authorities in EU Member States.

The PSD2 was adopted by the European Parliament on 25 November 2015. This directive is an extension of the First Payment Services Directive (PSD1, Directive 2007/64/EU) published in 2007. The deadline for the Member States to transpose the directive into their national legislation was January 13, 2018.

The directive introduces fundamental changes in the payment service industry, such as third party access to bank infrastructures, transparency of user information, security of personalised security credentials, traceability of payment transactions, monitoring of security incidents, major incident reporting, etc.

The PSD2 reinforces the security of technological uses to ensure the confidentiality, integrity and availability of sensitive payment data, for which it is necessary to implement a framework for operational risk management and security with the following security measures:

- Awareness of the payment service users
- Consent of consumers
- Strong customer authentication
- Authentication code with dynamic link
- Dedicated interface
- Monitoring of security measures

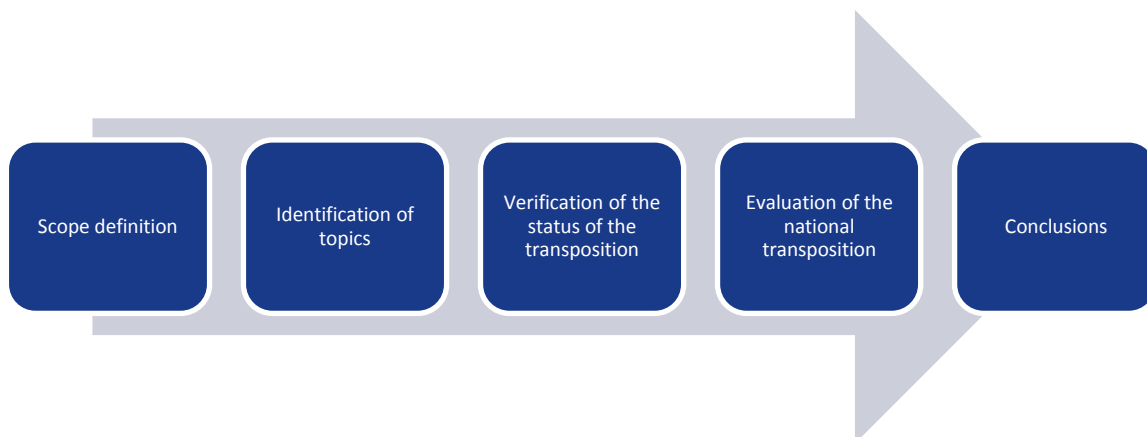
The PSD2 requires that all payment service providers notify security incidents in order to promote good risk management practices and ensure that information is shared between the public and private sectors:

- Operators' essential services in the financial sectors
- Public entities of incident response centres
- Public administrations

² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>

1.3 Methodology

This study was carried out using a five-step methodology that begins with the definition of the scope. Then it moves on to the initial stage of identification of the essential aspects of the Payment Services Directive. The third and fourth steps include the verification of the transposition of the PSD2 into the national legislation of the Member States and an evaluation of the transposition. Finally, the study ends with conclusions.



- **Scope definition:** The first step was to establish the structure, objectives, and focus of the project.
- **Identification of topics:** Identification and in-depth analysis of the most important topics of the directive.
- **Verification of the status of the transposition:** Analysis of the status of the transposition in the different Member States of the EU.
- **Analysis of the national transposition:** Comparison of the requirements of the national transposition of Member States with respect to the original directive.
- **Conclusions:** As a result of the activities described here, the information obtained was organised and developed into this document, using the information gathered during the desktop research and following the structure found in the index of this document. The final step was to check the content, making sure that the information was reliable and accurate.

1.4 Structure of the document

This document is structured as follows:

- **Chapter 1. Introduction:** Brief presentation of the report, listing the objectives defined and describing the methodology followed.
- **Chapter 2. Dimension of the report:** List of the different actors and services involved in the transposition of the PSD2 into the 28 Member States of the European Union.
- **Chapter 3. Overview of the implementation of the PSD2:** General analysis of the state of the strategy into the 28 Member States of the European Union.
- **Chapter 4. Current state of PSD2 transposition in EU Member States:** General analysis of the state of the strategy in the 28 Member States of the European Union.
- **Chapter 5. Good practices on PSD2 transposition:** Most common aspects analysed in the transpositions and graphs of the results obtained.

1.5 Source of data and information

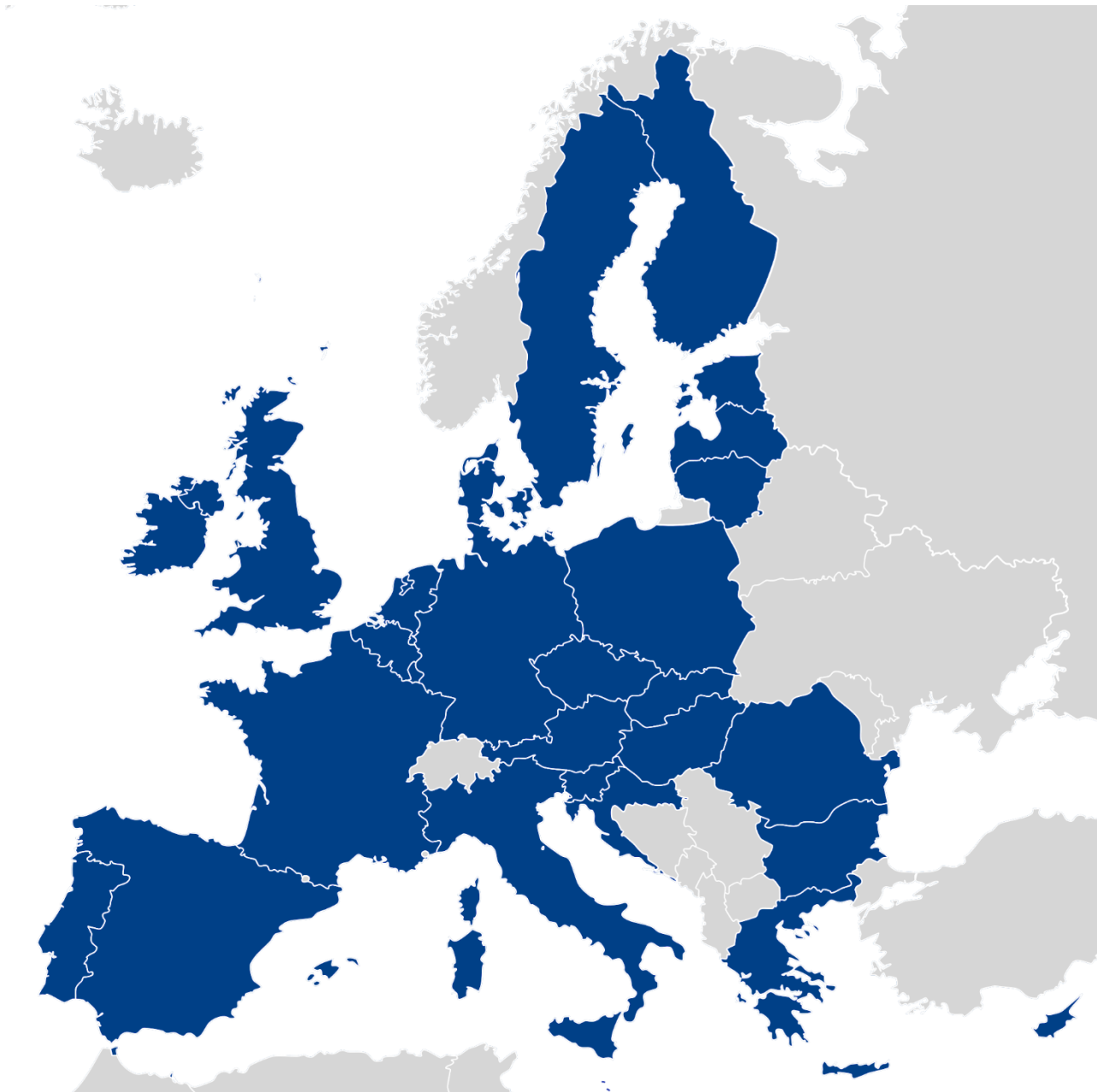
The sources of the data and the information gathered to develop the study are as follows:

- Publications and comments made by EBA
- Other reports published by ENISA

- Publications and comments from the competent authorities of the EU Member States
- Directives, regulatory technical standards, and guidelines of the PSD2

1.6 Scope of the report

The Member States involved in the study are the **28 Member States** of the European Union. At the time of publication, most of the Member States have completed the transposition of the PSD2, not full transposition is in the [Netherlands](#), [Portugal](#) and [Romania](#).



1.7 Types of actors

In each Member State, there will be one or several competent authorities, who will oversee and guarantee the operation of the directive between financial entities of the Member States and the cross-border cooperation with the EBA and ECB:

- [Competent authorities](#) grant authorisations to exercise the financial tasks, control and decide on the possibility of revoking the authorisations granted.

- [Competent supervisory authorities](#) monitor compliance with the directive by payment institutions, empowering them to exercise fundamental rights.
- [Competent notification authorities](#) receive periodic notifications from payment service providers about updated assessments of operational and security risks, statistical data of payment transactions made, and serious incidents identified.
- [Competent sanctioning authorities](#) impose sanctions in case of infringement of the provisions of national law resulting from the transposition.

The following European competent authorities are also included, to whom national authorities should provide information on payment services:

- The [European Banking Authority \(EBA\)](#) guarantees fair competition in that market, avoiding unjustifiable discrimination against any existing player in the market.
- The [European Central Bank \(ECB\)](#) is responsible for overseeing the banking system and regulating the money stock in an economy.
- The [European Union Agency for Network and Information Security \(ENISA\)](#) is the centre of expertise for cybersecurity in Europe.

2. Overview of the implementation of the PSD2

2.1 Current Status by Member States

This section presents the information obtained on how the different EU Member States approach the implementation of the PSD2 and the contact information of the competent national authorities.

The scope of this study includes the analysis of cybersecurity topics in the payment service environments issued by the following entities:

- The [European Parliament](#) and the [Council of the European Union](#), the PSD2 and the regulatory technical standards of Article 98.1 (PSD2);
 - Second Payment Services Directive (Directive (EU) 2015/2366³);
 - Article 98.1 (PSD2): Regulatory Technical Standards (RTS) for strong customer authentication (SCA) and common and secure open standards of communication (Regulation (EU) 2018/389⁴);
- The [European Banking Authority](#), the good practice guidelines of Articles 95.3 and 96.3 of the PSD2;
 - Article 95.3 (PSD2): Security measures for operational and security risks of payment services (EBA/GL/2017/17⁵)
 - Article 96.3 (PSD2): Major incident reporting (EBA/GL/2017/10⁶)

The RTS of Article 98.1 of the PSD2 is a commission delegated regulation of the [European Parliament and the Council](#), so there is no need for transposition and it is directly enforceable.

On the other hand, the guidelines published by the [EBA](#) require confirmation of compliance by the Member States. If the countries comply with the EBA guidelines, they can apply the guidelines published by the EBA directly or adapting them to the national law.

Compliance with the directive requires the supervision of the Competent Authorities. In the area of cybersecurity, most of the EU Member States (MS) have a Computer Security Incident Response Team (CSIRT). At the European level, there is the [European Union Agency for Network and Information Security \(ENISA\)](#), operational since 1 September 2005. ENISA is a centre of expertise for cybersecurity in Europe, contributing to a high level of network and information security in the EU, developing and promoting a culture of cybersecurity in society to help the proper functioning of the internal market. Finally, at the national level, there are competent national authorities for supervision, monitoring, and reporting of major incidents.

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389>

⁵ https://www.eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_EN.pdf/c63cfcfb-7412-4cfb-8e07-47a05d016417

⁶ <http://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf>

COUNTRY	ENTRY INTO FORCE	NATIONAL LAW	COMPETENT AUTHORITY	SUPERVISION AUTHORITY	INCIDENT REPORTING AUTHORITY
Austria	01 June 2018	Federal Act on the Provision of Payment Services 2018 https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00332/imfname_672716.pdf	Financial Market Authority https://www.fma.gv.at/		
Belgium	26 March 2018	Service Public Federal Finances https://www.nbb.be/doc/cp/moniteur/2018/20180303_wet_26_03_2018.pdf http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&pub_date=2018-07-30&numac=2018031489&caller=summary	National Bank of Belgium https://www.nbb.be/en		
Bulgaria	06 March 2018	Law on Payment Services and Payment Systems http://www.bnb.bg/bnbweb/groups/public/documents/bnb_law/laws_payment_services_en.pdf	Bulgarian National Bank http://www.bnb.bg/		
Croatia	18 July 2018	Law on Payment Transactions https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_66_1330.html Law on Electronic Money https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1304.html	Croatian National Bank for credit institutions http://www.hnb.hr/ Croatian Financial Services Supervisory Agency for investment firms https://www.hanfa.hr/	Croatian Financial Services Supervisory Agency	Croatian National Bank
Cyprus	18 April 2018	The provision and use of payment services and access to payment systems law N. 31(I)/2018 https://www.centralbank.cy/images/media/pdf_el/Payment%20Systems%20Law%20GR%2018042018.pdf	Central Bank of Cyprus https://www.centralbank.cy/		
Czech Republic	13 January 2018	Payment System Act No. 370/2017 https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislative/zakony/download/zakon_370_2017.pdf	Czech National Bank https://www.cnb.cz/cs/index.html		
Denmark	01 January 2018	Act on payments 652 of 08/06/2017 https://www.finanstilsynet.dk/~media/Lovgivning/Lovsamling/2018/LOV-652-af-080617-pdf.pdf	Financial Supervisory Authority (FSA) https://www.finanstilsynet.dk/		
Estonia	13 January 2018	The Law on Payment Institutions and Electronic Money Institutions https://www.riigiteataja.ee/en/eli/ee/531012018007/consolidate#	Financial Supervision Authority https://www.fi.ee		

COUNTRY	ENTRY FORCE	INTO	NATIONAL LAW	COMPETENT AUTHORITY	SUPERVISION AUTHORITY	INCIDENT REPORTING AUTHORITY
			Law of Obligations Act https://www.riigiteataja.ee/akt/107122017005			
Finland	13 January 2018		Payment Services Act (HE 132/2017 vp) https://www.eduskunta.fi/FI/vaski/HallituksensEsitys/Documents/HE_132+2017.pdf Payment Institutions Act (HE 143/2017 vp) https://www.eduskunta.fi/FI/vaski/HallituksensEsitys/Documents/HE_143+2017.pdf	Financial Supervisory Authority http://www.fin-fsa.fi/en/pages/default.aspx		
France	31 August 2018		Monetary and Financial Code https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026&dateTexte=20180525	Prudential Supervisory Authority and Resolution (ACPR) https://acpr.banque-france.fr/		
Germany	13 January 2018		Law implementing the Second Payment Services Directive https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze/Gesetzesvorhaben/Abteilungen/Abteilung_VII/18_Legislaturperiode/2017-07-21-Umsetzung-Zweite-Zahlungsdienstrichtlinie/3-Verkuendetes-Gesetz.pdf;jsessionid=EFFEDFE8FF7FC602F869DB0DEF94D783?__blob=publicationFile&v=2	Federal Financial Supervisory Authority https://www.bafin.de/EN/Homepage/homepage_node.html		
Greece	13 January 2018		Law number 4537 https://www.bankofgreece.gr/BoGDocuments/%CE%9D_4537_2018_%CE%9184.pdf	Bank of Greece https://www.bankofgreece.gr		
Hungary	13 January 2018		T/17566a No. http://www.parlament.hu/irom40/17566/17566.pdf	Central Bank of Hungary https://www.mnb.hu/en		
Ireland	13 January 2018		European union (payment services) regulations 2018 http://www.finance.gov.ie/wp-content/uploads/2018/01/18012-S.I.-No.-6-of-2018-European-Union-Payment-Services-Regulations-2018.pdf	Central Bank of Ireland https://www.centralbank.ie/home		
Italy	13 January 2018		Legislative Decree 15 December 2017, n. 218 http://www.gazzettaufficiale.it/eli/gu/2018/01/13/10/sg/pdf	Bank of Italy http://www.bancaditalia.it/homepage/index.html		

COUNTRY	ENTRY FORCE	INTO	NATIONAL LAW	COMPETENT AUTHORITY	SUPERVISION AUTHORITY	INCIDENT REPORTING AUTHORITY
Latvia	13 July		Payment Services and Electronic Money Law https://likumi.lv/doc.php?id=206634	Financial and Capital Market Commission http://www.fktk.lv		
Lithuania	13 August 2018		Service Public Federal Finances https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/63e361e2488011e89197e1115e5dbece	Bank of Lithuania https://www.lb.lt/en/		
Luxembourg	29 July 2018		Official Journal of the Grand Duchy of Luxembourg N ° 612 From 25 July 2018 http://data.legilux.public.lu/file/eli-etat-leg-loi-2018-07-20-a612-jo-fr-pdf.pdf	Financial Sector Supervisory Commission http://www.cssf.lu/		
Malta	13 January 2018		Directive No. 1: The Provision and Use of Payment Services https://www.centralbankmalta.org/file.aspx?f=434 Chapter 376 Financial Institutions Act https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/Consultation/2018/Proposed%20Amendments%20to%20FIA.pdf	Central Bank of Malta https://www.centralbankmalta.org Malta Financial Services Authority https://www.mfsa.com.mt/	Central Bank of Malta https://www.centralbankmalta.org	
Netherlands			Amendment of the Act on Financial Supervision Act https://zoek.officielebekendmakingen.nl/dossier/34813/kst-34813-A?resultIndex=13&sorttype=1&sortorder=4	De Nederlandsche Bank https://www.dnb.nl		
Poland	31 Dec 2018		Act on payment services http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001075/O/D20181075.pdf	Polish Financial Supervision Authority https://www.knf.gov.pl/		
Portugal	13 Nov 2018		The national law of the PSD2 (English): Decree-Law No. 91/2018, of November 12 Decreto-Lei n.º 91/2018, de 12 de novembro https://www.bportugal.pt/sites/default/files/anexos/legislacoes/335415275_2.docx.pdf	Bank of Portugal https://www.bportugal.pt/		
Romania	26 March 2018		Draft legislative act Emergency Ordinance on Payment Services http://www.anpc.gov.ro/galerie/file/proiecte_acte/2018/oug_serviciile_de_plata.pdf	National Bank Romania http://www.bnr.ro/Home.aspx		

COUNTRY	ENTRY INTO FORCE	NATIONAL LAW	COMPETENT AUTHORITY	SUPERVISION AUTHORITY	INCIDENT REPORTING AUTHORITY
Slovakia	13 January 2018	Draft law 624/2017 https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=441236	National Bank of Slovakia https://nbs.sk/sk/titulna-stranka		
Slovenia	22 Feb 2018	Law on payment services, services for issuing electronic money and payment systems https://www.uradni-list.si/_pdf/2018/Ur/u2018007.pdf	Bank of Slovenia https://www.bsi.si/		
Spain	25 Nov 2018	Royal Decree-Law 19/2018, of November 23 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16036	Bank of Spain https://www.bde.es		
Sweden	01 May 2018	Service Public Federal Finances https://www.fi.se/contentassets/72e226a0abe14cecb44443fedd2f12c1/fs1804.pdf	Financial Supervisory Authority https://www.fi.se/sv/		
United Kingdom	13 August 2018	The Payment Services Regulations 2017 http://www.legislation.gov.uk/uksi/2017/752/pdfs/ukxi_20170752_en.pdf	Prudential Regulation Authority https://www.bankofengland.co.uk/Financial-Conduct-Authority(FCA) https://www.fca.org.uk/	Financial Conduct Authority (FCA)	

3. Good practices on the transposition of PSD2

This chapter presents an analysis of the state of the implementation of the PSD2 in the 28 Member States of the EU. The information presented here is accurate as of the date the study was finalised, i.e. September 2018.

3.1 Overview

The PSD2 is applicable since 13 January, 2018. Currently, almost all Member States have completed the transposition of the new directive, with only one country, expected to finalise the transposition in the beginning of 2019.

The Member States implement the PSD2 based on the national transposition procedures of the directives. Each state can apply a different implementation type, such as:

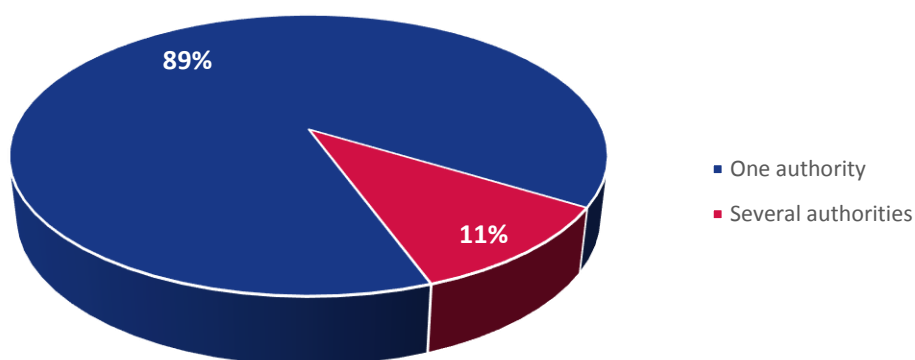
- Adapting the PSD2 to a new law and subrogating the current laws applied to payment services and electronic money.
- Updating the law of PSD1 with the new requirements of the PSD2.
- Modifying the current laws related to the requirements of the PSD2 in the appropriate domain.

3.1.1 Competent Authorities

The PSD2 requires Member States to establish competent authorities for the registration, authorisation, and supervision of payment service providers. Most MS have established the national central bank as the only competent authority, while other MS, in addition to the national central bank, also have financial authorities as their supervisory authorities. Examples include [Croatia](#) (National Bank for credit institutions and Financial Services Supervisory Agency for investment firms), [Germany](#) (Federal Financial Supervisory Authority and Bundesbank), and the [United Kingdom](#) (Prudential Regulation Authority and Financial Conduct Authority).

The authorities represented are valid only for PSD2 regulation. It should be noted, that other competent authorities might be involved on a national level, through other legislative means, such as Memorandum of Understanding, specific national legislation, and others.

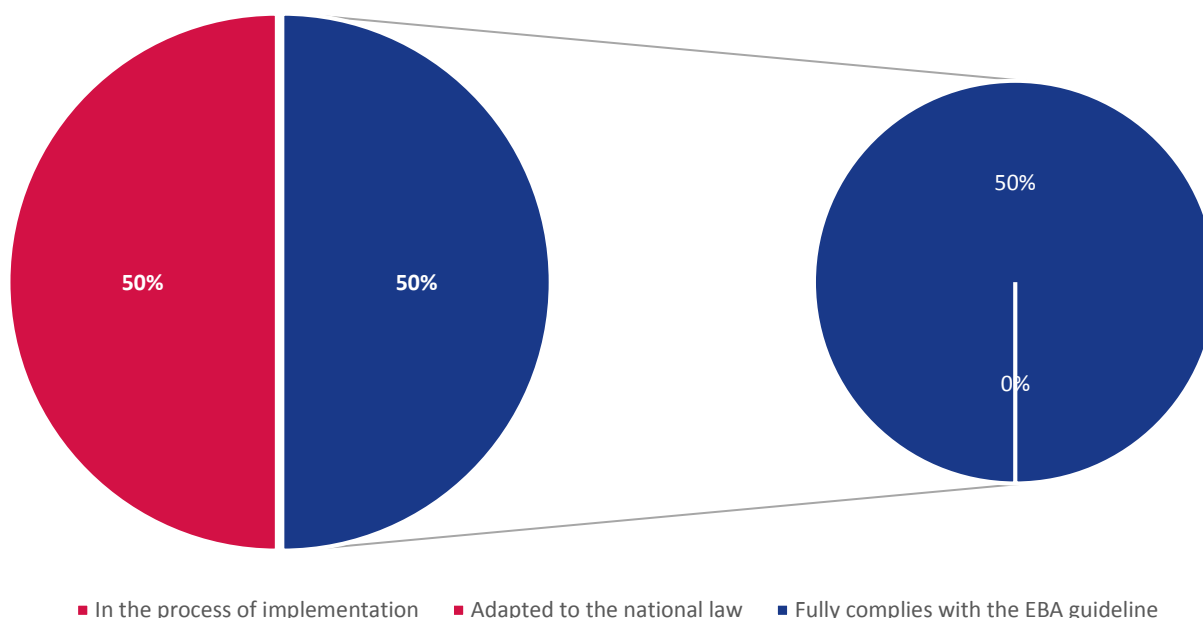
Graph 1. Number of competent authorities per country



3.2 Guidelines on the security measures for operational and security risks under PSD 2

The study carried out on the adaptation of the guideline on security measures for operational and security risks associated with payment services determined that most of the Member States will apply the guideline published by the EBA.

Graph 2. Guideline on the security measures adaptation status



Currently, only 50% of the countries have responded to how they will adapt the guideline on security measures, the rest are pending response. It is estimated that all countries will have made the adaptation before the end of the year 2018, with the exception of [Denmark](#), [Germany](#) and [Slovakia](#), which notified that the adaptation will take place in 2019.

The PSD2 requires PSPs to provide competent authorities with an updated and complete assessment of operational and security risks associated with payment services. All States have established an annual periodicity, but there are some that specify the delivery date, such as:

- [Estonia](#) requires PSPs to submit the evaluation once a year but no later than 1 March.
- [Latvia](#) and [Poland](#) require PSPs to submit the evaluation before 31 January.
- [Sweden](#) requires PSPs to submit the evaluation before 21 February.

3.2.1 Mapping of the PSD 2 security measures to the NIS Directive

The PSD 2 has guidelines on security and operational risks with measures proposed. The NIS directive defines minimum security measures grouped in security domains.

As PSD 2 covers payment service providers and the NIS Directive covers credit institutions, it will be useful to have a basic mapping of the security measures and controls to help both the regulators and the institutions.

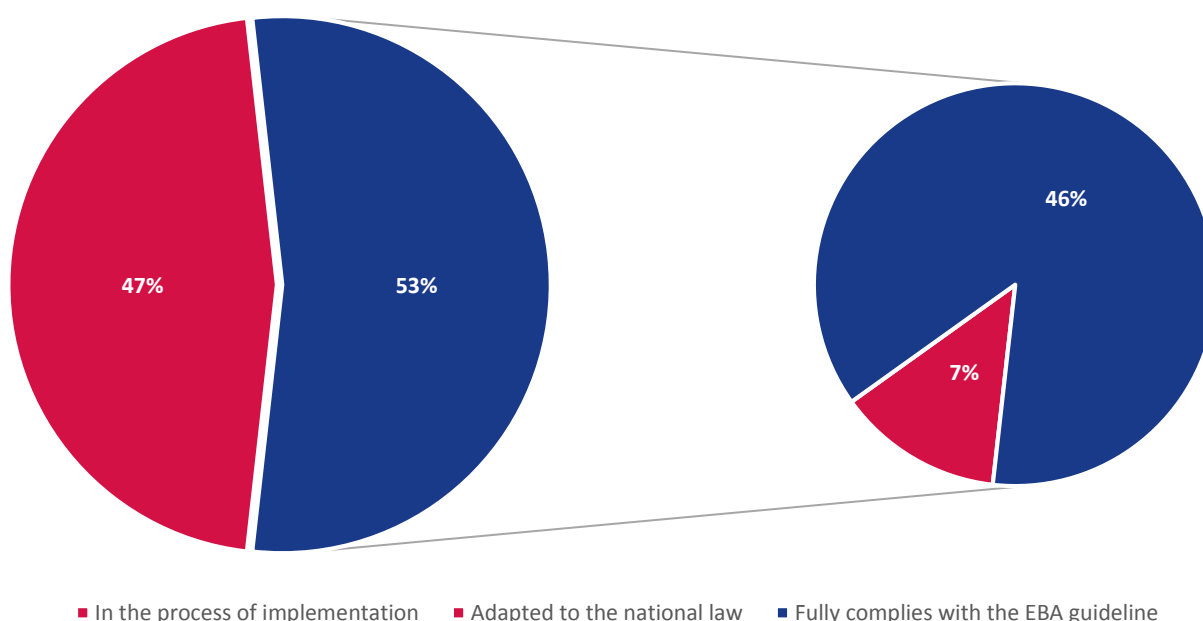
NIS DIRECTIVE			PSD2		
Security Domains	Security sub-domains	Security Measures	Guideline	Section	
1. Governance and Ecosystem	1.1 Information System Security Governance & Risk Management	1.1.1 Information system security risk analysis	Guideline 2: Governance. Guideline 3: Risk assessment	-Operational and security risk management framework -Risk management and control models -Outsourcing -Identification of functions, processes and assets. -Classification of functions, processes and assets -Risk assessments of functions, processes and assets	
		1.1.2 Information system security policy			
		1.1.3 Information system security accreditation			
		1.1.4 Information system security indicators			
		1.1.5 Information system security audit			
		1.1.6 Human resource security			
	1.2 Ecosystem Management	1.2.1 Ecosystem mapping	n/a		
		1.2.2 Ecosystem relations			
2. Protection	2.1 IT Security Architecture	2.1.1 Systems configuration	Guideline 4: Protection		
		2.1.2 System segregation			
		2.1.3 Traffic filtering	n/a		
		2.1.4 Cryptography			
	2.2 IT Security Administration	2.2.1 Administration accounts	Guideline 4: Protection	-Data and systems integrity and confidentiality	
		2.2.2 Administration information systems			
	2.3 Identity and access management	2.3.1 Authentication and identification	Guideline 4: Protection	-Access control	
		2.3.2 Access rights			
	2.4 IT Security Maintenance	2.4.1 IT security maintenance procedure	n/a		
		2.4.2 Industrial control systems			
	2.5 Physical and environmental security	2.5.1 Physical and environmental security	Guideline 4: Protection	-Physical security -Access control	
	3. Defence	3.1 Detection	3.1.1 Detection	Guideline 5: Detection	-Continuous monitoring and detection

		3.1.2 Logging	Guideline 8: Situational awareness and continuous learning	-Monitoring and reporting of operational or security incidents - Threat landscape and situational awareness - Training and security awareness programmes
		3.1.3 Logs correlation and analysis		
	3.2 Computer Security Incident Management	3.2.1 Information system security incident response	Guidelines on major incident reporting (EBA/GL/2017/10)	
		3.2.2 Incident Report		
		3.2.3 Communication with competent authorities and CSIRTs		
	4. Resilience	4.1.1 Business continuity management	Guideline 6: Business continuity	-Scenario-based business continuity planning -Testing of business continuity plans -Crisis communication
		4.1.2 Disaster recovery management	Guideline 7: Testing of security measures	
		4.2.1 Crisis management organization	n/a	
		4.2.2 Crisis management process		

3.3 Guideline on major incident reporting under PSD 2

With regard to the study of the adaptation of the guideline on major incidents reporting in Member States, it has been concluded that most states directly apply the document published by the EBA, while only 2 countries have adapted it to their national law ([Czech Republic](#) and [United Kingdom](#)).

Graph 3. Guideline on major incident reporting adaptation status

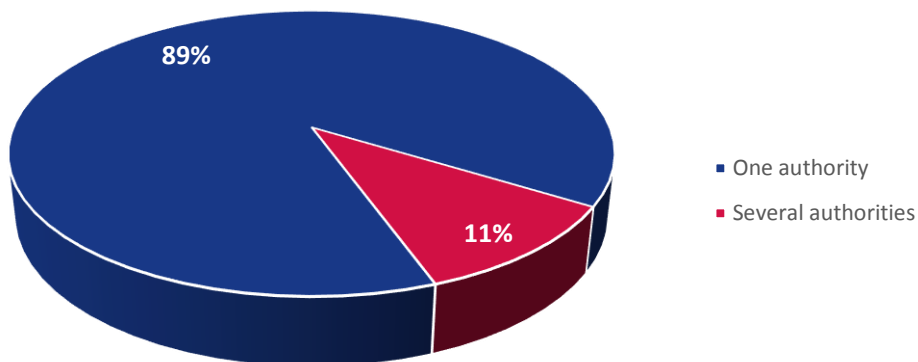


For more information on the status of the adaptation in each Member State, see **Annex 4.1 Compliance status with PSD2 Guidelines**.

3.3.1 Incident reporting authorities

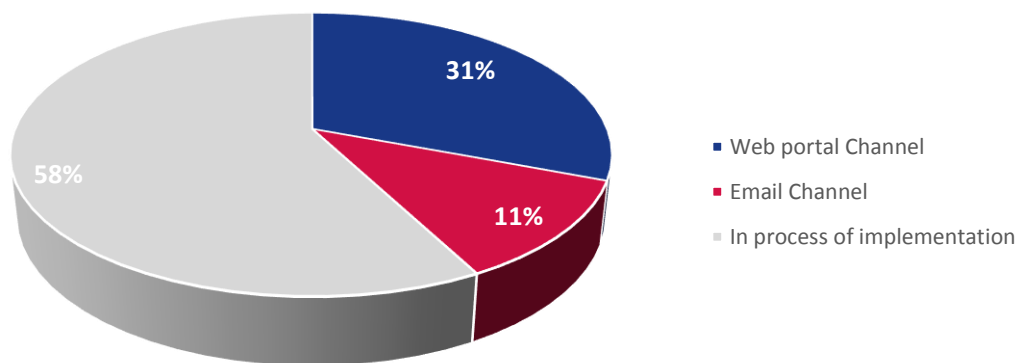
Most Member States have established a one competent authority for the supervision and notification of incidents, with the exception of [France](#), and [Malta](#), which require a parallel notification to the national central bank and the financial authority.

Graph 4. Member States with parallel communication



Each competent authority establishes a communication channel for the notification of incidents, which can be a web portal, email, telephone call, etc. Most authorities prefer the web portal channel, since it allows for greater traceability and management of incidents.

Graph 5. Incident Reporting Channel



The notifications through web portals require that PSPs be previously registered, so that the authorities can authenticate the providers that have sent the notifications and subsequently carry out a follow-up. The competent authorities that use web portals have published a user manual on the necessary procedures for the notifications of incidents.

3.3.2 Notification threshold

The competent authorities require PSPs to use the EBA templates to inform them of the incident. The template will be progressively completed in three phases: initial, intermediate and final.

- Phase I. Initial report
 - PSPs should send the initial report to the competent authority within **4 hours** from the moment the major operational or security incident was first detected.

- PSPs should also submit an initial report to the competent authority when a previously non-major incident becomes a major incident.
- PSPs should include headline-level information of the incident.
- PSPs should also include in their initial report the date for the next update, which should be as soon as possible and under no circumstances go beyond **3 business days**.
- **Phase II. Intermediate report**
 - PSPs should submit intermediate reports every time they consider that there is a relevant status update or by the date for the next update indicated in the previous report.
 - PSPs should submit to the competent authority a first intermediate report with a more detailed description of the incident and its consequences.
 - PSPs should indicate in each report the date for the next update, which should be as soon as possible and under no circumstances go beyond **3 business days**.
 - PSPs should send the last intermediate report when regular activities have been recovered and business is back to normal, informing the competent authority of this circumstance.
- **Phase III. Final report**
 - PSPs should send a final report when the root cause analysis has taken place and there are actual figures available to replace any estimates.
 - PSPs should deliver the final report to the competent authority within **a maximum of 2 weeks** after business is deemed back to normal.
 - PSPs should aim to include in their final reports full information.

Most states have followed the EBA notification guidelines. Some of the states have made minimal modifications:

- **Czech Republic**
 - It is not allowed to subcontract notifications of incidents
- **Italy⁷**

This is valid only for European significant institutions, under the SSM Incident reporting framework. For other institutions, a different incident reporting procedures are currently available⁸.

- The initial notification must be made before **2 hours** after the detection of the incidents.
- The intermediate notification must be made before **10 working days** from the previous notification.
- The final notification must be made within **20 working days** of the previous notification.
- **France and Malta**
 - Notify 2 competent authorities, National Central Bank and Supervision Authority.

Regarding the statistical data on fraud related to the different means of payment, Member States require PSPs to deliver them once a year, with the exception of **Sweden**, which will provide them once a semester, before 21 February and before 21 August.

⁷ This is valid only for European Significant Institutions, under the SSM Incident reporting framework.

⁸ <https://www.bancaditalia.it/statistiche/raccolta-dati/segnalazioni/rilevazioni-vigilanza/index.html>

3.3.3 Mapping of notification criteria of the PSD 2 and the NIS Directive

The PSD 2 and the NIS directive both have notification requirements, which in some cases might crossover each other. PSD 2 covers payment service providers and the NIS covers credit institutions, which in some cases might be the same institution.

PSD2 CRITERIA	NIS DIRECTIVE CRITERIA
PSUs affected	No. of users affected by the disruption of the essential service
Service downtime	Duration of the incident
Other PSPs or relevant infrastructures potentially affected	Geographical spread with regard to the area affected by the incident
Economic impact	Economic impact
Reputational impact	
High Level of internal escalation	
Transactions affected	

4. Annex A – Country Details

4.1 Austria

On 24 April, 2018, the Austrian Federal Ministry of Finance published federal legislation (Federal Law on the Provision of Payment Services 2018 - BGBl. I No. 17/2018) implementing the PSD2. The legislation enters into force on 1 June, 2018.

COUNTRY	AUSTRIA
Entry into Force	01 June 2018
National Transposition Law	Federal Act on the Provision of Payment Services 2018 https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00332/imfname_672716.pdf
Competent Authority	Financial Market Authority https://www.fma.gv.at/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	https://webhost.fma.gv.at/incomingplattform/ip.htm

4.1.1 Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

ZaDig §85. Handling operational and security-related risks

1. A PSP shall establish a framework of appropriate risk mitigation measures and control mechanisms to manage the operational and security risks associated with the payment services provided. As part of this framework, the PSP has to establish and apply effective incident handling procedures. This must include, in particular, the detection and classification of serious operational and security incidents.

2. The PSP shall provide the Financial Market Authority (FMA) annually with an updated and comprehensive assessment of the operational and security risks related to the payment services provided. In particular, the assessment shall indicate whether risk mitigation measures and control mechanisms taken to control risks are appropriate. The FMA may stipulate that the update of the valuation must be made at shorter intervals.

FMA comments⁹: The Financial Market Authority shall take into account European convergence in respect of supervisory tools and supervisory procedures in the enforcement of the provisions under national and European law. In this regard, the Guidelines and Recommendations and other measures passed by resolution that are issued by the European Banking Authority (EBA) must be applied. In addition, the warnings and recommendations passed by the European Systemic Risk Board (ESRB) must also be complied with.

These Guidelines derive from the mandate given to the EBA in Article 95(3) of Directive (EU) 2015/2366 (PSD2). These Guidelines specify requirements for the establishment; implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide.

Austria will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.1.2 Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

ZaDig §86. Reporting incidents

⁹ <https://www.fma.gv.at/en/eu/eba-guidelines/>

- (1) In the event of a serious operational or security incident, a PSP shall immediately inform the Financial Market Authority (FMA) in writing. If the incident affects or could affect the financial interests of its PSUs, the PSP shall immediately notify its PSUs of the incident. The notification must clarify any action that PSUs can take to limit the negative impact of the incident.
- (2) The FMA shall, upon receipt of a notification pursuant to paragraph 1, immediately inform EBA and the ECB of the relevant details of the incident. In cooperation with these authorities, the FMA has to examine the relevance of the incident to other relevant Union authorities and to inform them accordingly. After the FMA has examined the relevance of the incident to the relevant authorities, it also informs them accordingly. If necessary, the FMA must take all necessary precautions for the immediate safety of the financial system.
- (3) PSPs have provided the FMA with statistical data on frauds related to different means of payment once a year. The FMA must make these data available to the EBA and the ECB in an aggregated form.

Additional notes	PSPs shall inform the FMA in writing in the event of a serious security incident. Measures to mitigate security incidents delivered to users shall be clear.
Incident reporting channel	https://webhost.fma.gv.at/incomingplattform/ip.htm

FMA Comments¹⁰: The Financial Market Authority shall take into account European convergence in respect of supervisory tools and supervisory procedures in the enforcement of the provisions under national and European law. In this regard, the Guidelines and Recommendations and other measures passed by resolution that are issued by the European Banking Authority (EBA) must be applied. In addition, the warnings and recommendations passed by the European Systemic Risk Board (ESRB) must also be complied with.

These Guidelines derive from the mandate given to the EBA in Article 96(3) of 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 (PSD2).

In particular, these Guidelines specify the criteria for the classification of major operational or security incidents by PSPs as well as the format and procedures they should follow to communicate, as laid down in Article 96(1) of the above-mentioned directive, such incidents to the CA in the home MS.

In addition, these Guidelines deal with the way these CAs should assess the relevance of the incident and the details of the incident reports that, according to Article 96(2) of the said directive, they shall share with other domestic authorities.

Moreover, these Guidelines also deal with the sharing with the EBA and the ECB of the relevant details of the incidents reported, for the purposes of promoting a common and consistent approach.

4.1.3 Regulatory Technical Standards on authentication and communication

AUSTRIA

ZaDig §4. For the purposes of this Federal Law, the following definitions apply:

47. Secure communication: a communication procedure that complies with the requirements of Commission Delegated Regulation (EU) 201X / XX of XX. XXXX 201X complies with SCA and shared and secure communication under Article 98 of Directive (EU) 2015/2366;

4.2 Belgium

On 11 March, 2018, the National Bank of Belgium published federal legislation (Service Public Federal Finances 2018 - BELGISCH STAATSBLAD, 29444. 26/03/2018) implementing the PSD2. The legislation enters into force on 26 March, 2018.

COUNTRY	BELGIUM
Entry into Force	26 March 2018
National Transposition Law	Service Public Federal Finances https://www.nbb.be/doc/cp/moniteur/2018/20180303_wet_26_03_2018.pdf
Competent Authority	National Bank of Belgium

¹⁰ <https://www.fma.gv.at/en/eu/eba-guidelines/>

COUNTRY	BELGIUM
Supervision Authority	https://www.nbb.be/en
Incident Reporting Authority	
Incident Reporting Channel	https://onegate-certificate.nbb.be

4.2.1 Belgium: Guidelines on the Security Measures

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

Belgium will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.2.2 Belgium: Guidelines on Major Incident Reporting

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

Belgium will comply with the guideline on major incident reporting issued by the EBA.

4.2.3 Belgium: Regulatory Technical Standards on authentication and communication

BELGIUM

9.1. Principle

Art. 46. § 1. Pls register, monitor and restrict access to and keep track of sensitive payment data in accordance with the provisions of the RTS adopted by the European Commission pursuant to Article 98 of the Directive (EU) 2015/2366.

§ 2. For the purposes of paragraph 1, Pls shall comply in particular with the rules referred to in Articles 47 and 48.

9.2. Authentication - General Obligations

Art. 47. § 5. The measures taken pursuant to paragraphs 1 to 3 comply with the RTS adopted by the European Commission pursuant to Article 98 (1) (a) and (c) of Directive (EU) 2015 / 2366.

§ 6. Pls may derogate from paragraphs 1 to 3 subject to compliance with the conditions established by the RTS adopted by the European Commission pursuant to Article 98 (1) (b) and (3) of the Directive (EU) 2015/2366.

Subsection 10. - Secure Communication

Art. 49. Pls comply with common open and secure communication standards for the purposes of identification, authentication and reporting of information, as well as for the implementation of security measures, between service providers, account management payment services, payment initiation service providers, account information service providers, payers, payees and other payment service providers in accordance with RTS pursuant to Article 98 (1) (d) of Directive 2015/2366 (EU).

11.2. Measures to protect users against security risks

Art. 51. Pls shall take measures to ensure adequate protection of PSUs against identified security risks, including fraud and the misuse of sensitive or personal data. The measures they apply comply with the conditions laid down by the RTS adopted by the European Commission pursuant to Article 98 (2) of Directive (EU) 2015/2366.

4.3 Bulgaria

On 6 March, 2018, the Bulgarian National Bank published federal legislation (Law on Payment Services and Payment Systems) implementing the PSD2. The legislation enters into force on 6 March, 2018.

COUNTRY	BULGARIA
Entry into Force	06 March 2018
National Transposition Law	Law on Payment Services and Payment Systems http://www.bnb.bg/bnbweb/groups/public/documents/bnb_law/laws_payment_services_en.pdf

COUNTRY	BULGARIA
Competent Authority	Bulgarian National Bank http://www.bnb.bg/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.3.1 Bulgaria: Guidelines on the Security Measures

STATUS	IN PROCESS OF IMPLEMENTATION
<p>EBA comments²: <i>Intends to comply</i>. By the end of the first half of 2018.</p> <p>Bulgaria will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.</p>	

4.3.2 Bulgaria: Guidelines on Major Incident Reporting

STATUS	IN PROCESS OF IMPLEMENTATION
<p>EBA comments⁴: <i>Intends to comply</i>. It is envisaged by the end of the first half of 2018 the Bulgarian National Bank to adopt the relevant regulations, internal rules and procedures implementing the requirements of the Guidelines.</p> <p>Bulgaria will comply with the guideline on major incident reporting issued by the EBA.</p>	

4.3.3 Bulgaria: Regulatory Technical Standards on authentication and communication

BULGARIA
<p>Article 71. Confirmation on the Availability of Funds</p> <p>(2) The PSP issuing payment instruments may request confirmation under paragraph 1 provided that all of the following conditions are met:</p> <p>3. the PSP issuing payment instruments authenticates itself towards the ASPSP before each confirmation request, and securely communicates with the ASPSP in accordance with the requirements specified in a delegated act adopted by the European Commission under Article 98, paragraph 4 of Directive (EU) 2015/2366.</p> <p>Article 72. Access to a Payment Account in the Case of PISs</p> <p>(3) The PSP shall:</p> <p>4. when providing PISs, authenticate itself towards the ASPSP and securely communicate with him, the payer and the payee in accordance with the requirements specified in a delegated act adopted by the European Commission under Article 98, paragraph 4 of Directive (EU) 2015/2366;</p> <p>(4) The ASPSP shall: 1. communicate securely with PSPs in accordance with the requirements specified in a delegated act adopted by the European Commission under Article 98, paragraph 4 of Directive (EU) 2015/2366;</p> <p>Article 73. Access to and Use of Payment Account Information in the Case of AISs</p> <p>(2) The AISP shall:</p> <p>3. when communicating, authenticate itself towards the ASPSP and securely communicate with him and the PSU in accordance with the requirements specified in a delegated act adopted by the European Commission under Article 98, paragraph 4 of Directive (EU) 2015/2366;</p>

4.4 Croatia

On 18 and 20 July, 2018, legislation (Payment System Act and Electronic Money Act) implementing the PSD2 was published. The legislation entered into force on 26 July 2018 (Electronic Money Act) and on 28 July 2018 (Payment System Act).

COUNTRY	CROATIA
Entry into Force	26 July 2018/ 28 July 2018
National Transposition Law	Law on Payment Transactions https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_66_1330.html Law on Electronic Money https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1304.html
Competent Authorities	Croatian National Bank for credit institutions http://www.hnb.hr/
Supervision Authority	Croatian National Bank http://www.hnb.hr/ Ministry of Finance – the Financial Inspectorate http://www.mfin.hr/hr/financijski-inspektorat additional authorities: Ministry of Economy, Entrepreneurship and Crafts https://www.mingo.hr/ Croatian Regulatory Authority for Network Industries https://www.hakom.hr/
Incident Reporting Authority	Croatian National Bank
Incident Reporting Channel	Croatian National Bank: psd2.incident@hnb.hr

4.4.1 Croatia: Guidelines on the Security Measures

Payment System Act²: Article 67 Operational and security risk and authentication(2) PSPs are required to fulfil their obligations under paragraph 1 of this Article in accordance with the Guidelines of the European Supervisory Authority on Banking for Operational and Security Risk-Related Security Measures pursuant to Directive (EU) 2015/2366 (EBA/GL/2017/17).

Croatia complied with the guideline on the security measures for operational and security risks of payment services issued by the EBA as the necessary legislative proceedings have been completed.

4.4.2 Croatia: Guidelines on Major Incident Reporting

Payment System Act⁴: Article 68 incident reporting (1) The PSPs referred to in Article 7, paragraph 1, item 1, sub-item (a) and (c), item 2, sub- item a), item 3, item 4, sub -item a), item 5 and item 6 sub-item (a) they are obliged to notify the Croatian National Bank of any significant operational or safety incident without delay and in accordance with the Guidelines of the EBA on Reporting of Major Incidents pursuant to Directive (EU) 2015/2366 (EBA/GL/2017/10)

Croatia complied with the guideline on the security measures for operational and security risks of payment services issued by the EBA as the necessary legislative proceedings have been completed.

4.4.3 Croatia: Regulatory Technical Standards on authentication and communication

CROATIA

Article 35 Confirmation of availability of funds

(1) A PSP issuing a payment instrument based on a card may send an available availability payment request to the PSP that is responsible for the amount required to execute the payment transaction based on the card available in the payment account of the payer only if all of the following conditions are met:

3. A PSP issuing a payment instrument based on a card shall authenticate to the PSP who accounts prior to each availability request and communicates with it in a secure manner in accordance with Delegated Commission Regulation (EU) 2018/389 of 27 November 2017. (EU) No 2015/2366 of the European Parliament and of the Council as regards RTS for reliable SCA and common and secure open standards for communication (OJ L 69, 13.3.2018, hereinafter referred to as: Regulation (EU) No 2018/389).

Article 36 Rules for access to a payment account in the case of a PIS

(3) PISP:

5. upon each payment initiation, it shall confirm its identity with the PSP who keeps the account in accordance with Regulation (EU) No. 2018/389

6. it is obliged to communicate with the PSP which manages the account, the payer and the payee in a secure manner, in accordance with Regulation (EU) No. 2018/389

(4) For the purpose of securing the right of the payer to use the PIS and provided that the payer has given his explicit consent to execute a payment transaction in accordance with Article 34 of this Act, the PSP managing the account shall:

1. It is obliged to communicate in a secure manner with PIS providers in accordance with Regulation (EU) No. 2018/389

2. immediately upon receipt of the payment order from the PIS provider, make or make available to the PISP all information on the initiation and any information regarding the execution of the payment transaction available to it in accordance with Regulation (EU) No. 2018/389

Article 37 Rules of access and use of payment account information in the case of account information

(3) AISP:

4. It must confirm its identity with the PSP who accounts with the account or a number of such providers at each communication session in accordance with Regulation (EU) No. 2018/389

5. it is obliged to communicate with the PSP managing the account or with a large number of such providers and the PSU in a safe manner, in accordance with Regulation (EU) No. 2018/389

(4) The PSP holding the account:

1. it is obliged to communicate in a secure manner with the AISP, in accordance with Regulation (EU) No. 2018/389

Article 69 Authentication

(7) PSP are obliged to apply the provisions of this Article in accordance with Regulation (EU) No. 2018/389.

4.5 Cyprus

On 18 April, 2018, the Central Bank of Cyprus published federal legislation (The provision and use of payment services and access to payment systems law N. 31(I)/2018) implementing the PSD2. The legislation enters into force on 18 April, 2018.

COUNTRY	CYPRUS
Entry into Force	18 April 2018
National Transposition Law	The provision and use of payment services and access to payment systems law N. 31(I)/2018 https://www.centralbank.cy/images/media/pdf_el/Payment%20Systems%20Law%20GR%2018042018.pdf
Competent Authority	
Supervision Authority	Central Bank of Cyprus https://www.centralbank.cy/
Incident Reporting Authority	
Incident Reporting Channel	SD.InfoSecurity@cengtralbank.cy

COUNTRY	CYPRUS
	Jst.cyboe@centralbank.cy

4.5.1 Cyprus: Guidelines on the Security Measures

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

EBA comments²: *Intends to comply*. By such time as the necessary legislative or regulatory proceedings have been completed, and the PSD2 is transposed into national law.

4.5.2 Cyprus: Guidelines on Major Incident Reporting

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

EBA comments⁴: *Intends to comply*. By such time as the necessary legislative or regulatory proceedings have been completed, that is when the PSD2 is transposed into national law.

Cyprus will comply with the guideline on major incident reporting issued by the EBA.

4.5.3 Cyprus: Regulatory Technical Standards on authentication and communication

CYPRUS

65.- Confirmation of availability of funds

(2) The PSP may request the confirmation referred to in subsection (1) if the following conditions are cumulatively met:

(c) the PSP verifies his identity to the user's account service payment service provider prior to each confirmation request and communicates securely with his ASPSP in accordance with the RTS referred to in Article 98 (1) , point (d) of Directive (EU) 2015/2366 and approved in accordance with Article 98 (4) of that Directive.

66.-Rules for accessing a payment account in the case of start-up payment services.

(3) The PSP must

(d) whenever the initiation of payments is made, identify itself with the payee's PSP and communicate in a secure manner with the PSP, payer and payee in accordance with the RTS referred to in Article 98 (1) (d) of Directive (EU) 2015/2366 and approved in accordance with Article 98 (4) of that Directive;

(4) The PSP shall be required to

(a) communicate securely with PSPs in accordance with the RTS referred to in Article 98 (1) (d) of Directive (EU) 2015/2366 and approved in accordance with Article 98 (4) of that Directive;

67.-Rules for accessing and using payment account information in the case of AIS

(2) The AISP shall,

(c) for each communication cycle, be identified with the PSU's PSP (s) and communicate securely with the account service provider (s) and PSU (s) in accordance with RTS referred to in Article 98 (1) (d) of Directive (EU) 2015/2366 and approved in accordance with Article 98 (4) of that Directive;

(3) In relation to payment accounts, the PSP must

(a) communicate securely with AISPs in accordance with the RTS referred to in Article 98 (1) (d) of Directive (EU) 2015/2366 and approved in accordance with Article 98 (4) of that Directive;

4.6 Czech Republic

The National Bank of Czech Republic published federal legislation (Payment System Act No. 370/2017) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	CZECH REPUBLIC
Entry into Force	13 January 2018

COUNTRY	CZECH REPUBLIC
National Transposition Law	Payment System Act No. 370/2017 https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislativa/zakony/download/zakon_370_2017.pdf
Competent Authority	Czech National Bank https://www.cnb.cz/cs/index.html
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	https://oam.cnb.cz/sipresextdad/SIPREEXT.www_forms.login?p_lan=CS&p_sk=UVI

4.6.1 Czech Republic: Guidelines on the Security Measures

Czech National Bank comments²: On 12 January 2018, the European Banking Authority (EBA) issued the authorization referred to in Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009 / EC and repealing Commission Decision 2009/78 / EC, hereinafter referred to as the "Regulation establishing the EBA" - EBA General Guidelines on Security Measures relating to Operational and Security Risks for Payment Services under Directive) 2015/2366 (PSD2) (EBA/GL/2017/17, external link) (the "Guidelines").

Under Article 16 (3) of the EBA, the competent authorities and financial market participants must make every effort to comply with these guidelines and recommendations. **The Czech National Bank has confirmed, in accordance with Article 16 (3) of the EBA, which it intends to follow these guidelines.**

The Czech Republic will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.6.2 Czech Republic: Guidelines on Major Incident Reporting

Czech National Bank comments⁴: On 27 July 2017, the European Banking Authority (EBA) issued the authorization referred to in Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (EBA), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC - hereinafter referred to as "the Regulation establishing an EBA" - Guidelines on the notification of major incidents under Directive (EU) 2015/2366 on payment services market (PSD2) (EBA/GL/2017/10, external link) (the "Guidelines").

Under Article 16 (3) of the EBA, the competent authorities and financial market participants must make every effort to comply with these guidelines and recommendations. The Czech National Bank has confirmed, in accordance with Article 16 (3) of the EBA, which it intends to follow these guidelines.

Supervisory authorities shall lay down the conditions under which it is appropriate for notified incidents to be shared with other authorities in the country, and similar conditions shall be set for sharing incidents with EBA and the ECB, including general guidelines for communication.

Czech Republic will comply with the guideline on major incident reporting issued by the EBA.

4.6.3 Czech Republic: Regulatory Technical Standards on authentication and communication

CZECH REPUBLIC

Section 223 Strong user authentication

(5) The method of strong user authentication referred to in subsections (1) and (2) is provided for by the directly applicable European Union regulation implementing Article 98 of Directive 2015/2366 of the European Parliament and of the Council.

CZECH REPUBLIC

(6) Subsections (1) and (2) do not apply to cases laid down under the directly applicable European Union regulation implementing Article 98 of Directive 2015/2366 of the European Parliament and of the Council.

Section 225 Relation to a directly applicable European Union regulation

The person authorised to provide payment services provides payment services in accordance with a directly applicable European Union regulation implementing Article 98 of Directive 2015/2366 of the European Parliament and of the Council.

Section 278

The provisions of Sections 223 and 225 apply for the first time 18 months after the effective date of the directly applicable European Union regulation implementing Article 98 of Directive (EU) 2015/2366 of the European Parliament and of the Council.

4.7 Denmark

The Danish law implementing PSD2 was adopted by the Danish Parliament on 8 June 2017, and came into force on 1 January 2018.

COUNTRY	DENMARK
Entry into Force	01 January 2018
National Transposition Law	Law on Payments https://www.retsinformation.dk/forms/r0710.aspx?id=191823
Competent Authority	Financial Supervisory Authority (FSA) https://www.finanstilsynet.dk/
Supervision Authority	Danish Competition and Consumer Authority https://www.en.kfst.dk/
Incident Reporting Authority	The office of the Consumer Ombudsman https://www.consumerombudsman.dk/
Incident Reporting Channel	Reporting mail channel: Financial Supervisory Authority ⁵ (Finanstilsynet) ITincidents@ftnet.dk

4.7.1 Denmark: Guidelines on the Security Measures

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

EBA comments²: *Intends to comply.* By 01.01.2019.

4.7.2 Denmark: Guidelines on Major Incident Reporting

Danish Financial Supervisory Authority comments: Companies covered by the Act on Payments must inform Finanstilsynet as soon as possible of major operational and safety incidents, cf. section 127 (1). 1 in the same law. The detailed requirements for what the reporting should contain is set out in EBA's Guidelines on Reporting of Important IT Events.

Danish Executive Order on the subject, which will be in force on 1 January 2019 (link in Danish) – <https://www.retsinformation.dk/eli/lt/2018/1428>

4.7.3 Denmark: Regulatory Technical Standards on authentication and communication

DENMARK

Section 126. A PSP must determine and maintain

3) appropriate safeguards that protect the integrity and confidentiality of the user's personal security measures in accordance with regulations and rules issued by the Commission pursuant to Article 98 of Directive 2015/2366 / EU of the European Parliament and of the Council of 25 November 2015 on payment services in the interior market.

Section 128. A PSP shall use strong customer authentication unless otherwise provided by regulations and rules issued by the Commission pursuant to Article 98 of Directive 2015/2366 / EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market when a user

1) Access their payment account online,

2) initiates an electronic payment transaction or

3) Carries out actions through a remote communication device that may pose a risk of abuse.

Section 129. The Minister of Enterprise may lay down rules necessary to apply or implement the decisions or acts adopted by the Commission pursuant to Article 98 of Directive 2015/2366 / EU of the European Parliament and of the Council of 25 November 2015 on payment services in the inner market.

4.8 Estonia

On 13 January, 2018, the Estonian Financial Supervision Authority published federal legislation (The Law on Payment Institutions and Electronic Money Institutions) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	ESTONIA
Entry into Force	13 January 2018
National Transposition Law	The Law on Payment Institutions and Electronic Money Institutions https://www.riigiteataja.ee/en/eli/ee/531012018007/consolide# Law of Obligations Act https://www.riigiteataja.ee/akt/107122017005
Competent Authority	Financial Supervision Authority https://www.fi.ee
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	https://www.fi.ee/index.php?id=19910

4.8.1 Estonia: Guidelines on the Security Measures

FSA comments²: To issue the EBA an indicative guide to the Financial Supervision Authority "Guidelines for the operation and security of payment services under Directive (EU) 2015/2366 (PSD2)" the security measures to be used "(EBA/GL/2017/17);

2. publish the guidelines referred to in point 1 on the website of the Financial Supervision Authority together with the English language the original text;

3. The coordinator of international cooperation to confirm to the EBA that The Financial Supervision Authority intends to comply fully with the guidelines referred to in point 1.

4. The guidelines referred to in paragraph 1 shall apply from the date of adoption of this Decision.

Estonia will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.8.2 Estonia: Guidelines on Major Incident Reporting

FSA comments⁴: 1. issue guidance from the EBA as an indicative guide to the Financial Supervision Authority Guidelines on Notification of Significant Incidents in accordance with Directive (EU) 2015/2366 (EBA/GL/2017/10) from the transposition of Directive (EU) 2015/2366 into Estonian law and to the extent that in accordance with applicable national law;
2. publish the guideline mentioned in clause 1 on the website of the Financial Supervision Authority;
3. The coordinator of international cooperation to confirm to the EBA that The Financial Supervision Authority intends to comply with the guidelines referred to in point 1 as from Directive (EU) 2015/2366 transposition into Estonian law and to the extent consistent with applicable national law.

Estonia will comply with the guideline on major incident reporting issued by the EBA.

4.8.3 Estonia: Regulatory Technical Standards on authentication and communication

ESTONIA

The Law on Payment Institutions and Electronic Money Institutions (RT I, 07.12.2017, 2)

§ 132. Alignment of activities and documents of payment institutions and electronic money institutions with the entry into force of this Act, which came into force on January 13, 2018

(5) Persons who provided PIS or AIS in Estonia for the purposes of this Act before 12 January 2016 may continue to provide these services until the entry into force of the European Commission's implementing regulation referred to in Article 98 of Directive 2015/2366/EU of the European Parliament and of the Council, in accordance with 2018 By the regulation in force on the entry into force of the 13 January edition.

(6) PSPs with whom a client has a payment account may not restrict access to a client's payment account by the PIS and the PSP of the AIS on the grounds that they do not implement the European Commission's implementing regulation referred to in Article 98 of Directive 2015/2366/EU of the European Parliament and of the Council.

Law of Obligations Act (RT I, 07.12.2017, 5)

§ 724.4. Approval and limitation of funds

(5) The PSP, with whom the payer has a payment account, at the payer's request, at the request of the payer, provide the identification code of the PSP that issued the card payment instrument and confirmation of the existence of the required amount of money for the payer.

(6) If the payment is initiated by or through a card-based payment instrument and the exact amount of the payment transaction is not known to the payer at the time the transaction is authorized, the PSP of the payer may block the amount of money in the payer's payment account only if the latter has given consent to block a specific amount of money.

(7) The PSP shall release the amount of money from the blockage specified in subsection (6) of this section without delay after the exact amount of the payment, but at the latest upon receipt of the payment order.

(8) The PSP requesting the validation of the required amount of money shall provide the PSP with whom the customer has a payment account with information allowing him to be identified each time before the application is submitted.

[RT I, 07.12.2017, 1 - entered into force. Sections 5 and 8 of 13.01.2018 enter into force 18 months after the adoption of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market, Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repeal of Directive 2007/64/EC (OJ L 337, 23.12.2015, pp. 35-127) - Entry into force of the Commission Implementing Regulation referred to in Article 98.]

§ 724.5. Providing PIS and AIS

(3) The PIS and the PSP that provides the AIS shall provide the PSP with whom the customer has a payment account with information allowing him to be identified each time before the payment is initiated or submission of an account information request.

[RT I, 07.12.2017, 1 - entered into force. 13.01.2018, paragraph 3 will enter into force 18 months after the adoption of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market, Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093 / 2010 and the repeal of Directive 2007/64/EC (OJ L 337, 23.12.2015, pp. 35-127) - Entry into force of the Commission Implementing Regulation referred to in Article 98.]

§ 724.6. Implementation of security requirements by the PSP

(1) PSPs shall use a secure way of communicating upon the authentication and provision of the services specified in § 724.4 and 724.5 of this Act and shall implement security measures that ensure the confidentiality of personalized security features and integrity of data.

(2) The specific requirements for the secure communication and security measures specified in subsection (1) of this section shall be established by the European Commission Implementing Regulation referred to in Article 98 of Directive 2015/2366/EU of the European Parliament and of the Council.

(3) A PSP requires a SCA whenever a payer wishes to access his payment account online, initiates an electronic payment transaction, or makes any other transaction that results in the risk of misuse or fraudulent use of the payment service information, provided for in this Act, or other legislation does not provide otherwise.

ESTONIA

(4) A PSP uses a SCA in an electronic payment transaction initiated through an Internet connection or other remote access, including a payment transaction initiated through a PIS, in a manner that involves a component through which a payment transaction can be dynamically linked to a flat payment amount and to the payee.

[RT I, 07.12.2017, 1 - entered into force. 18 months after the adoption of Directive 2015/2366/EU of the European Parliament and of the Council 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 Directive 2007/64 //EC repealed (OJ L 337, 23.12.2015, pp. 35-127) - entry into force of the Commission Implementing Regulation referred to in Article 98.]

§ 727.1. Information on the execution of a payment order under a one-time payment service agreement

(1) Upon receipt of a payment order submitted on the basis of a single payment service agreement, the payer's PSP shall without delay provide to the payer, in the manner provided for in subsection 711 (2) of this Act, the following information:

- 1) the number of the payment order or other identifier that allows the payment transaction to be identified and information on the recipient, if applicable;
- 2) the amount of money to be transferred in the currency expressed in the payment order;
- 3) the amount of fees payable by the payer and, if applicable, information on the basis for the formation of the fees or their distribution;
- 4) if applicable, the exchange rate or base rate, if it differs from the provision submitted pursuant to subsection 711.1 (1) 4) of this Act, and the amount of the amount transferred after the conversion of that currency;
- 5) the date of receipt of the payment order.

[RT I 2010, 2, 3 - entered into force. 22.01.2010]

(5) Upon receipt of a payment order, the PSP shall make available to the PSP through which the payment order was initiated information on the initiation of a payment transaction and the execution of the transaction specified in subsection (1) of this section.

[RT I, 07.12.2017, 1 - entered into force. 18 months after the adoption of Directive 2015/2366/EU of the European Parliament and of the Council 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 Directive 2007/64 //EC repealed (OJ L 337, 23.12.2015, pp. 35-127) - entry into force of the Commission Implementing Regulation referred to in Article 98.]

4.9 Finland

The Finnish Financial Supervisory Authority published federal legislation (Payment Services Act (HE 132/2017 vp) and Payment Institutions Act (HE 143/2017 vp)) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	FINLAND
Entry into Force	13 January 2018
National Transposition Law	Payment Services Act (HE 132/2017 vp) https://www.eduskunta.fi/FI/vaski/HallituksEnesitys/Documents/HE_132+2017.pdf Payment Institutions Act (HE 143/2017 vp) https://www.eduskunta.fi/FI/vaski/HallituksEnesitys/Documents/HE_143+2017.pdf
Competent Authority	Financial Supervisory Authority http://www.fin-fsa.fi/en/pages/default.aspx
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting web channel: Financial Supervisory Authority http://www.fin-fsa.fi/en/pages/default.aspx

4.9.1 Finland: Guidelines on the Security Measures

Financial Supervisory Authority's comments: The most significant changes to Regulations and guidelines 8/2014 relate to management of payment service providers' operational and security risks as well as reporting of major payment service incidents. The FIN-FSA recommends that payment service providers comply with the EBA's Guidelines on the Security Measures for

Operational and Security Risks of Payment Services under PSD2 (EBA/GL/2017/17). Payment service providers shall also submit annually to the FIN-FSA a free-form assessment of the operational and security risks of payment services. The first assessment shall be submitted for 2018 by 28 February 2019. Incidents relating to operational and security risks of payment services shall be reported in accordance the EBA Guidelines (EBA/GL/2017/10), adhering to major incident classifications and reporting deadlines. A reporting form will be available on the FIN-FSA website.

Finland will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.9.2 Finland: Guidelines on Major Incident Reporting

Financial Supervisory Authority's comments: The most significant changes to Regulations and guidelines 8/2014 relate to management of payment service providers' operational and security risks as well as reporting of major payment service incidents. The FIN-FSA recommends that payment service providers comply with the EBA's Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2 (EBA/GL/2017/17). PSPs shall also submit annually to the FIN-FSA a free-form assessment of the operational and security risks of payment services. The first assessment shall be submitted for 2018 by 28 February 2019. Incidents relating to operational and security risks of payment services shall be reported in accordance the EBA Guidelines (EBA/GL/2017/10), adhering to major incident classifications and reporting deadlines. A reporting form will be available on the FIN-FSA website.

Finland has not made changes with respect to the requirements of the EBA guidelines.

4.9.3 Finland: Regulatory Technical Standards on authentication and communication

FINLAND

(HE 132/2017 vp) Section 85b Identification

The new paragraph to be added to Chapter 10 (some provisions and entry into force) would provide for the obligation of the PSP to use SCA in accordance with Articles 97 and 98 of the Directive. SCA is defined in Section 8, paragraph 24 of the Act.

Paragraph 4 stipulates that the SCA referred to in subsections 1 and 2 and the security measures referred to in subsection 3 shall meet the more stringent requirements set out in the Commission's RTS referred to in Article 98 of the Payment Services Directive. Pursuant to Article 98 (1) (a) and (c) of the Directive, the EBA shall draw up draft standards for those standards, which shall be submitted for approval by the Commission in accordance with Article 4. (B), secures and maintains fair competition between all PSPs (1), (2) and point (c)), ensure technological neutrality and business neutrality (point (d)) and enable the development of user-friendly and innovative payment methods that are readily available (point (e)). In order to revise the standards in the development of technology and business models, Article 5 provides that the EBA will regularly review them and update them as necessary.

According to Article 98 (1) (b) of the Directive, the Commission's RTS also specify the exceptions to the application of Article 97 (1) to (3) of the Directive, namely exceptions to the obligation of SCA and the protection of the confidentiality and integrity of personal identification numbers. This is proposed to be provided for in paragraph 5 of the law, which stipulates that the obligations under section 1-3 may be waived if the Commission's RTS so provide. According to Article 98 (3) of the Directive, exceptions must be based on the level of risk (a) of the service provided, the number of transactions, the frequency or both (point (b)) and the payment channel used for the execution of the payment transaction (c). The intention is that the unreasonably heavy identification requirements would prevent, for example, the development of near pay. The exceptions referred to here also apply to what has been said above for the general preparation and purpose, acceptance and review of standards.

(HE 132/2017 vp) Section 85c Communication Standards

This paragraph would provide for the obligation of the PSP to comply with common and secure open standards for communication with other PSPs, payers and payees in their contacts on the identification, authentication, disclosure, disclosure and security measures, the requirements of which are laid down in the Commission's RTS issued under Article 98 (1) (d). The preparation and the purpose of the standards, the adoption and the review are concerned with the provisions of Article 85 (2), (4) and (5) of the Directive. Article 65 (2) (c), Article 66 (3) (d) and (4) (a) and Article 67 (2) (c) and (3) (a) of the Directive refer to Article 95 (1) (d).

4.10 France

On 10 August, 2018, the French public service of the diffusion of right published federal legislation (Monetary and Financial Code) implementing the PSD2. The legislation enters into force on 31 August, 2018.

COUNTRY	FRANCE
Entry into Force	31 August 2018
National Transposition Law	Monetary and Financial Code https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026&dateTexte=20180525
Competent Authority	
Supervision Authority	Prudential Supervisory Authority and Resolution (ACPR) https://acpr.banque-france.fr/
Incident Reporting Authority	
Incident Reporting Channel	Reporting mail channel: ACPR and the Bank de France Notifications à la Banque de France ⁶ 2323-NOTIFICATIONS-UT@banque-france.fr

4.10.1 France: Guidelines on the Security Measures

The Prudential Supervisory Authority comments²: The Prudential Supervisory Authority has declared itself in compliance with the guidelines of the EBA (EBA/GL/2017/17) on security measures for operational and security risks related to payment services in the field of Directive (EU) 2015/2366 (PSD2). These guidelines are applicable to payment service providers - credit institutions, payment institutions and electronic money institutions - who must make every effort to comply with them, in accordance with the provisions of Article 16 of Regulation (EU) No 1093 / 2010 of the European Parliament and the Council of 24 November 2010 establishing the EBA.

France will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.10.2 France: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Art. L. 521-10.-I.-PSPs shall inform the Authority of Prudential Control and Resolution of any major operational incident without undue delay.

II.-PSPs shall inform the Bank de France without undue delay of any major security incident. The Bank de France shall evaluate the incident and, if necessary, take appropriate measures and, if it considers it necessary, inform the French Prudential Supervisory Authority pursuant to Article L. 631-1.

III.-Where the incident has or is likely to affect the financial interests of its payment service users, the PSP shall inform its PSUs of the incident without undue delay and any available measures they can take to mitigate the harmful effects of the incident.

IV.-Upon receipt of the notification referred to in I or II, the Prudential Supervisory Authority and the Bank of France shall without undue delay communicate the important details of the incident to the EBA and to the ECB and, having assessed the relevance of the incident for other national authorities concerned, inform them accordingly.

V.-The terms of the notifications provided for in I to III are specified by order of the Minister of Economy and Finance.

Additional Notes

France has transposed, in the Monetary and Financial Code article L.521-10, article 96 (1) (notify to the competent authorities about major incidents) and (2) (notify to the EBA and the ECB the details of the incidents). And the procedure of the PSP to provide, at least once a year, statistical data on fraud to the CAs, has been delegated to the Ministry of Economy and Finance.

The Prudential Supervisory and Resolution Authority's comments⁴: The Prudential Supervisory and Resolution Authority has complied with the guidelines of the EBA (EBA/GL/2017/10) on reporting of major incidents under Directive (EU) 2015/2366 (PSD2).

	<p>These guidelines specify, in particular, the criteria for the classification of major operational or security incidents by PSPs as well as the format and procedures that PSPs will have to apply in order to inform the Prudential Supervisory Authority of these incidents. Resolution and the Bank de France pursuant to the provisions of Article L. 521-10 of the French Monetary and Financial Code. These guidelines are applicable to PSPs - credit institutions, payment institutions and electronic money institutions - who must make every effort to comply with them, in accordance with the provisions of Article 16 of Regulation (EU) No 1093 / 2010 of the European Parliament and the Council of 24 November 2010 establishing the EBA. Incident notifications prepared using the model provided for in Appendix 1 of the guidelines should be sent to the Prudential Supervisory Authority and the Bank de France using the procedure available on the websites of the two authorities.</p>
	<p>France adopts the requirements of the EBA's guideline on major incident reporting and publishes a user manual on the notification of incidents.</p>

4.10.3 France: Regulatory Technical Standards on authentication and communication

FRANCE
<p>Article L133-39 I. - When the payment is initiated by means of a card-based payment instrument, the ASPSP, at the request of one of the PSP issuing the instrument, shall immediately confirm if the amount required to execute the card-related payment transaction is available on the payer's payment account, provided that all of the following conditions are met: 3 ° The PSP shall authenticate with the ASPSP before each request for confirmation and communicate with the ASPSP in accordance with the conditions laid down in the delegated act adopted pursuant to of Article 98.1 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 referred to above.</p> <p>Article L133-40 II. - When providing the PIS mentioned in point 7 of II of Article L. 314-1, the PSP: 4 ° Identify with the PSP managing the payer's account each time a payment is initiated and communicated under the conditions laid down in the delegated act adopted pursuant to Article 98.1 of the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 referred to above with the PSP account manager, the payer and the payee;</p> <p>Article L133-41 II. - When providing the AIS, the PSP: 3 ° identify himself, for each communication session, with the PSP(s) account managers of the PSU and communicate securely in accordance with the conditions laid down in the delegated act adopted pursuant to Article 98.1 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 referred to above with the accountant PSP(s) and the PSU;</p>

4.11 Germany

On 17 July, 2017, the German Federal Financial Supervisory Authority published federal legislation (Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 48, ausgegeben zu Bonn am 21. Juli 2017) implementing the PSD2. The legislation enters into force on January 13, 2018.

COUNTRY	GERMANY
Entry into Force	13 January 2018
National Transposition Law	<p>Law implementing the Second Payment Services Directive https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/18_Legislaturperiode/2017-07-21-Umsetzung-Zweite-Zahlungsdienstrichtlinie/3-Verkuendetes-Gesetz.pdf;jsessionid=EFFEDFE8FF7FC602F869DB0DEF94D783?__blob=publicationFile&v=2 </p>
Competent Authority	<p>Federal Financial Supervisory Authority https://www.bafin.de/EN/Homepage/homepage_node.html </p>

COUNTRY	GERMANY
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting web channel: Federal Financial Supervision Authority ⁵ (MVP portal) https://portal.mvp.bafin.de/MvpPortalWeb/app/login.html?locale=en_UK

4.11.1 Germany: Guidelines on the Security Measures

STATUS	IN PROCESS OF IMPLEMENTATION
--------	------------------------------

BaFin comments²: By 31.03.2019. BaFin intends to integrate the content of the Guidelines into the existing national rulebook for IT-supervision to avoid duplications of and possible contradictions with existing regulatory requirements. The necessary regulatory procedures should be completed by 31.03.2019 at the latest.

4.11.2 Germany: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

§ 54 Report of serious operational or security incidents

(1) A PSP must immediately inform the Federal Authority of a serious operational or security incident. The Federal Authority shall inform the EBA and the ECB immediately after receipt of a report on the relevant details of the incident. It must immediately examine the relevance of the incident for other domestic authorities with jurisdiction and inform them accordingly.

(2) The Federal Authority shall contribute to the examination by the EBA and the ECB of the relevance of the incident for other CAs of the European Union, the other MSs and the other Contracting States to the Agreement on the European Economic Area.

(3) If the Federal Authority is informed by the EBA or the ECB about an incident within the meaning of subsection (1) sentence 1, it shall take the necessary precautions for the immediate safety of the financial system.

(4) Where an incident within the meaning of the first sentence of paragraph 1 may affect the financial interests of its PSUs, a PSP shall immediately notify them of the incident and inform them of any action they may take to address the adverse effects of the incident limit.

(5) The PSPs shall provide the Federal Authority at least once a year with statistical data on cases of fraud in connection with the different means of payment. The Federal Authority shall make the submitted data available to the EBA and the ECB in aggregated form.

(6) Notification obligations of PSPs to other domestic authorities, cooperation tasks of the Federal Authority and the responsibilities of other domestic authorities for serious operational or security incidents remain unaffected.

Additional Notes	Germany requires PSPs to notify the Federal Authority without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Germany requires PSPs to provide the Financial Markets Authority, once a year, with statistical data on fraud involving different means of payment.
	Comments⁴: The new reporting procedure for major incidents in payment transactions, which replaces the previous reporting procedure pursuant to the minimum requirements for the security of internet payments (Mindestanforderungen an die Sicherheit von Internetzahlungen – MaSI), can be used already. As of 13 January, major incidents should only be reported using the new reporting templates and via BaFin's reporting and publishing platform (MVP Portal). <u>The EBA has also published guidelines regarding the question of when a security incident is regarded as major and therefore subject to the reporting requirement (see BaFinJournal August 2017 (only available in German)). BaFin intends to apply these guidelines, without any changes to the content, to German supervisory practice by means of a circular.</u> Payment service

	<p>providers subject to the reporting requirement should already follow the criteria specified in the guidelines.</p> <p>Germany has published the report “Creation of notifications of operating and security incidents in payment transactions” that specifies how to report security incidents. PSPs may rely on the indications in this report to prepare the necessary documentation to report to the competent authorities. The PSPs will notify the CAs through an XML file.</p>
	<p>Germany will comply with the requirements of the EBA guideline and will not make any changes.</p> <p>Germany has published a user manual report on how to create incident notifications and the necessary parameters to notify.</p> <p>The respective circular adopting the guidelines can be found on BaFin website¹¹</p>

4.11.3 Germany: Regulatory Technical Standards on authentication and communication

GERMANY

§ 46 Rights and obligations of the card issuing PSP

The card-issuing PSP may request the ASPSP for confirmation under § 45 (1) if the payer

1. gives the card-issuing PSP its explicit consent in advance and
2. triggered the card-based payment transaction for the amount in question using a card-based payment instrument issued by the card-issuing PSP.

The card issuing PSP must authenticate to the account providing PSP prior to each individual request for confirmation and to communicate with it in a secure manner. The card issuing PSP may not save the reply under § 45 (2) or use it for purposes other than the execution of the card-based payment transaction. For details, the delegated act is governed by Article 98 of Directive (EU) 2015/2366.

§ 48 Obligations of the ASPSP in the case of PIS

(3) The delegated act is further regulated by Article 98 of Directive (EU) 2015/2366.

§ 49 Obligations of the PISP

(6) The delegated act is further regulated by Article 98 of Directive (EU) 2015/2366.

§ 50 Obligations of the ASPSP for account information services

(3) The delegated act is further regulated by Article 98 of Directive (EU) 2015/2366.

§ 51 Obligations of the AISP

(4) The delegated act is further regulated by Article 98 of Directive (EU) 2015/2366.

§ 55 Strong Customer Authentication

(5) Details of requirements and procedures for SCA, including any exceptions to their application, and requirements for security arrangements for the confidentiality and integrity of the personalized security features are set out in a delegated act.

4.12 Greece

On 15 May, 2018, the Greek Newspaper of Government published legislation (Prefecture Number 4537) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	GREECE
Entry into Force	13 January 2018
National Transposition Law	<p>Law number 4537</p> <p>https://www.bankofgreece.gr/BoGDocuments/%CE%9D_4537_2018_%CE%9184.pdf</p>
Competent Authority	Central Bank of Greece

¹¹

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2018/rs_1808_Meldung_Zahlungssicherheitsvorfaelle.html

COUNTRY	GREECE
Supervision Authority	https://www.bankofgreece.gr
Incident Reporting Authority	
Incident Reporting Channel	sec.itsupervision@bankofgreece.gr

4.12.1 Greece: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

CHAPTER 5 OPERATIONAL RISKS, SAFETY RISKS AND IDENTIFICATION

Article 94 Managing operational and security risks (Article 95 of Directive 2015/2366/EU)

1. PSPs shall establish a framework with appropriate risk mitigation measures and control mechanisms to manage the operational and security risks associated with the payment services they provide. As part of this framework, PSPs shall establish and maintain effective incident management procedures, including for identifying and classifying major operational and security incidents.
2. PSPs shall provide the Bank of Greece, on a yearly basis or at shorter intervals specified by it, an up-to-date and comprehensive assessment of the operational risks and security risks associated with the payment services provided and the adequacy of the risk mitigation measures and the control mechanisms in place to address these risks.

Additional Notes

Greece requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.

Greece requires PSPs to provide the Bank of Greece with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.

EBA comments²: *Intends to comply.* By such time as the necessary legislative or regulatory proceedings have been completed.

4.12.2 Greece: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

CHAPTER 5 OPERATIONAL RISKS, SAFETY RISKS AND IDENTIFICATION

Article 95 Event reporting (Article 96 of Directive 2015/2366/EU)

1. In the event of a major operational event or security incident, PSPs established in Greece shall notify it without undue delay to the Bank of Greece. If the event affects or is likely to affect the financial interests of its PSUs, the PSP shall without undue delay notify its PSUs of the event and of any measures it may take to reduce the adverse effects of the incident.
2. Upon receipt of the notification provided for in paragraph 1, the Bank of Greece shall without undue delay provide the relevant details of the incident to the EBA and the ECB and, after assessing the relevance of the incident to the responsibilities of other authorities in the home country, shall inform the latter accordingly. In addition, the Bank of Greece cooperates with EBA and the ECB to assess the relevance of the incident to the competences of other EU and national authorities. If the Bank of Greece becomes a recipient of a disclosure referred to in paragraph 1 or a corresponding disclosure by EBA or the ECB, it shall, where appropriate, take all necessary measures to protect the immediate security of the domestic financial system.
3. PSPs operating in Greece shall provide the Bank of Greece, at least on a yearly basis, with statistics on fraud in the various payment instruments. The Bank of Greece shall transmit the data in question to the EBA and the ECB in aggregated form.

Additional Notes

Greece requires PSPs to notify the Bank of Greece without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform

	them of the mitigating measures to mitigate the incidence. Measures to mitigate security incidents delivered to users shall be clear. Greece requires PSPs to provide the Bank of Greece, at least on a yearly basis, with statistical data on fraud involving different means of payment.
	STATUS In process of implementation
	Comments⁴: Intends to comply. By such time as the necessary legislative or regulatory proceedings have been completed.

4.12.3 Greece: Regulatory Technical Standards on authentication and communication

GREECE	
Article 65 Confirmation of the availability of funds	
2. The PSP may request confirmation of the availability of the funds referred to in paragraph 1 if all the following conditions are met:	
(c) the PSP verifies his identity to the ASPSP prior to any request for confirmation of the availability of funds and communicates securely with his ASPSP in accordance with the Commission's delegated European Commission Regulation is issued in accordance with paragraph (d) of Article 98 (1) of Directive 2015/2366 / EU.	
Article 66 Rules for access to a payment account in the case of a PIS	
3. The PSP shall have the following obligations:	
(d) every time a payment is initiated, it shall verify its identity with the payer's PSP and communicate in a secure manner with the PSP, payer and payee in accordance with paragraph 1 of Article 98 of Directive 2015/2366 / EU,	
4. The ASPSP shall have the following obligations: (a) to communicate securely with PSPs in accordance with paragraph (d) of Article 98 of Directive 2015/2366 / EU,	
Article 67 Rules for access to and use of payment account information in the event of use of an AIS	
2. The AIS provider shall have the following obligations:	
(c) for each communication session, verify its identity with the PSU's PSP (s) or service provider (s) and communicate securely with the ASPSP (s) and PSU (s) in accordance with (d) of Article 98 (1) of Directive 2015/2366 / EU,	
3. The ASPSP shall have the following obligations regarding payment accounts: (a) communicate securely with AISPs, in accordance with paragraph (d) of Article 98 of Directive 2015/2366 / EU	

4.13 Hungary

In September 2017, the Central Bank of Hungary published federal legislation (T/17566a No.) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	HUNGARY
Entry into Force	13 January 2018
National Transposition Law	T/17566a No. http://www.parlament.hu/irom40/17566/17566.pdf
Competent Authority	Central Bank of Hungary https://www.mnb.hu/en
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting web channel: National Bank of Hungary ERA https://era.mnb.hu/ERA.WEB/

4.13.1 Hungary: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)	
--	--

IX / A. Chapter Operating and security risks, verification

55/A. § (1) The PSP shall set up a framework containing risk mitigation measures and control mechanisms in order to deal with the operational and security risks associated with the payment service provided by the PSP. As part of this framework, the PSP creates and maintains effective event management procedures, including the detection and classification of major operational and security incidents.

2. The PSP shall send an updated and comprehensive assessment to the HFSA of the operational and security risks associated with the payment service provided by it and the adequacy of the measures applied to mitigate these risks and the related control mechanisms once a year or at shorter intervals as determined by the Authority.

Additional Notes	Hungary requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Hungary requires PSPs to provide the Hungary Financial Supervision Authority with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.	
	STATUS	In process of implementation
	EBA comments ² : As at 13.03.2018, notification date. On 13th January 2018 MNB activated a notification portal so called ERA through which the PSPs can fulfil the reporting obligation relating to the operational and security risks assessment and mitigation measures implemented by them in accordance with Article 95(2) of Directive (EU) 2015/2366 (PSD2). PSPs were informed and are aware of the fact that the establishment of the framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide has to be done in accordance with the EBA Guidelines (EBA/GL/2017/17) published on the EBA website. Furthermore on the basis of the EBA Guideline Hungary will enhance the compulsory nature of the establishment of such a framework by issuing MNB Guidelines addressed to PSPs by 30.05.2018.	

4.13.2 Hungary: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

57. § IX / A. Chapter Operating and security risks, verification

55 / B. § (1) The PSP shall immediately inform the Supervisory Authority of the occurrence of a major operational or security incident.

2. Where a major operational or security event is likely to prejudice or prejudice the interests of the PSP's customers, the PSP shall, without undue delay, inform its customers of the event and of any measures available to mitigate the adverse effects of the event.

79. § (4a) The MNB shall inform it

(a) the European Banking Authority: ad) on the basis of information provided by payment service providers to the MNB on the aggregated statistical data on fraud related to different payment methods,

(b) the ECB: bb) on the aggregated statistical data on fraud related to different payment methods based on the information provided by the payment service providers to the MNB.

Additional Notes	Hungary requires PSPs to notify the Hungary Financial Supervision Authority without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Hungary requires PSPs to provide the Central Bank of Hungary (MNB) with statistical data on fraud involving different means of payment but it does not specify the periodicity of the delivery of the report.	
	STATUS	In process of implementation
	EBA comments ³ : Intends to comply. By 13.01.2019.	

The National Bank of Hungary includes a user manual⁵ detailing the incident reporting procedure.

4.13.3 Hungary: Regulatory Technical Standards on authentication and communication

HUNGARY

Article 58 The Pft. the following

66/A. Section 66 is added: "66 / A. § In the case of a payment initiative service or account information service, the Commission shall, for one year after the entry into force of the delegated regulation on Article 98 (1) (d) of the European Parliament and of the Council (EU) 2015/2366, but no later than 1 January 2019¹² until the payment service provider responsible for the client and its payment account is subject to the liability and liability rules of this Act as provided for by the provisions in force on 12 January 2018."

4.14 Ireland

In 2018, the Central Bank of Ireland published legislation (European Union (payment services) regulations 2018) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	IRELAND
Entry into Force	13 January 2018
National Transposition Law	European union (payment services) regulations 2018 http://www.finance.gov.ie/wp-content/uploads/2018/01/18012-S.I.-No.-6-of-2018-European-Union-Payment-Services-Regulations-2018.pdf
Competent Authority	Central Bank of Ireland https://www.centralbank.ie/home
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting web channel: Central Bank of Ireland https://onlinereporting.cbfsai.ie/Login?ReturnUrl=%2f

4.14.1 Ireland: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Section 118: Management of operational and security risks

(1) A PSP shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services that it provides.

(2) As part of the framework referred to in paragraph (1), a PSP shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(3) A PSP shall provide to the Bank on an annual basis, or at shorter intervals as determined by the Bank, an updated and comprehensive assessment of—

(a) the operational and security risks relating to the payment services provided by the PSP, and

(b) the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

¹² At time of writing, there is a modification procedure and text might change. http://www.parlament.hu/folyamatban-levo-torvenyjavaslatok?p_auth=kooYM228&p_p_id=pairproxy_WAR_pairproxyportlet_INSTANCE_9xd2Wc9jP4z8&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&pairproxy_WAR_pairproxyportlet_INSTANCE_9xd2Wc9jP4z8_pairAction=%2Finternet%2Fcplsql%2Fogy_irom.irom_adat%3Fp_ckl%3D41%26p_izon%3D2924

Additional Notes	<p>Ireland requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.</p> <p>Ireland requires PSPs to provide the Central Bank of Ireland with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.</p>
	<p>Comments²: (10 April 2018) On 12 December 2017, the European Banking Authority (EBA) published Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2). These Guidelines set out the requirements that payment service providers (PSPs) should implement in order to mitigate operational and security risks derived from the provision of payment services. The Guidelines cover governance, including the operational and security risk management framework, and risk management and control models, and outsourcing; risk assessment, including the identification and classification of functions, processes and assets; and the protection of the integrity and confidentiality of data and systems, physical security and access control. The Guidelines also cover the monitoring, detection and reporting of operational or security incidents; business continuity management, scenario-based continuity plans including their testing and crisis communication; the testing of security measures; situational awareness and continuous learning; and the management of the relationship with payment service users. In accordance with Article 16(3) of Regulation (EU) No 1094/2010, competent authorities and financial institutions must make every effort to comply with guidelines. <u>The Central Bank complies with the Guidelines and has incorporated them into its ongoing supervisory practices and processes for PSPs.</u> Firms are expected to comply with the Guidelines. The Guidelines are effective from 13 January 2018.</p>
	<p>Ireland will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.</p>

4.14.2 Ireland: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Section 119: Incident reporting

- (1) Where a major operational or security incident occurs, a PSP shall, without undue delay, notify the CA of its home MS.
- (2) Where an incident to which paragraph (1) applies has or may have an impact on the financial interests of the PSUs of the PSP concerned, the PSP shall, without undue delay, inform its PSUs of the incident and of all measures that those users can take to mitigate the adverse effects of the incident.
- (3) The Bank shall, following receipt of a notification referred to in paragraph (1), without undue delay, provide the relevant details of the incident to the EBA and to the ECB.
- (4) The Bank shall, following receipt of a notification referred to in paragraph (1) and after assessing the relevance of the incident concerned to relevant authorities of the State, notify those authorities accordingly.
- (5) Where the Bank receives a notification from the ECB under Article 96 of the Payment Services Directive, the Bank shall, on the basis of that notification, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.
- (6) A PSP shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to the CA of its home MS.
- (7) The Bank shall provide to the EBA and the ECB, in an aggregated form, data received under paragraph (6).

Additional Notes	<p>Ireland requires PSPs to notify the Central Bank of Ireland without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.</p> <p>Ireland requires PSPs to provide the Central Bank of Ireland, at least on an annual basis, with statistical data on fraud involving different means of payment.</p>
	<p>Comments⁴: (26 February 2018) On 27 July 2017 the European Banking Authority (EBA) published Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2). The Guidelines set out the criteria, thresholds and methodology to be used by payment service providers (PSPs) to determine whether or not an operational or security incident should be considered major and, therefore, be notified to the competent authority (CA) in the home Member State. In addition, these Guidelines establish the template that PSPs will have to use for this notification and the reports they have to send during the lifecycle of the incident, including the timeframes for submitting those reports. In accordance with Article 16(3) of</p>

	Regulation (EU) No 1094/2010, competent authorities and financial institutions must make every effort to comply with guidelines. <u>The Central Bank complies with the Guidelines and has incorporated them into its ongoing supervisory practices and processes for PSPs.</u> Firms are expected to comply with the Guidelines from their effective date of 13 January 2018.
	Ireland adopts the requirements of the EBA's guideline on major incident reporting and publishes a user manual ⁵ on the notification of incidents.

4.14.3 Ireland: Regulatory Technical Standards on authentication and communication

IRELAND

Confirmation on the availability of funds

89.(2) A PSP issuing card-based payment instruments may request the confirmation referred to in paragraph (1) where all of the following conditions are met:

(c) the PSP authenticates itself to the ASPSP concerned before each confirmation request, and securely communicates with the ASPSP in accordance with the RTS specifying the requirements referred to in point (d) of Article 98(1) of the PSD.

Rules on access to payment account in the case of PISs

90.(4) A PISP shall—

(d) on each occasion that a payment is initiated, identify itself to the ASPSP of a payer and communicate with the ASPSP, the payer and the payee concerned in a secure way, in accordance with the RTS specifying the requirements referred to in point (d) of Article 98(1) of the PSD,

(5) An ASPSP shall—

(a) communicate securely with a PISP in accordance with the RTS specifying the requirements referred to in point (d) of Article 98(1) of the PSD,

Rules on access to and use of payment account information in the case of AISs

91.(3) An AISP shall—

(c) for each communication session, identify itself to the ASPSP of the PSU concerned and securely communicate with the ASPSP and the PSU, in accordance with the RTS specifying the requirements referred to in point (d) of Article 98(1) of the PSD,

(4) An ASPSP shall, in respect of payment accounts—

(a) communicate securely with an AISP in accordance with the RTS specifying the requirements referred to in point (d) of Article 98(1) of the PSD,

4.15 Italy

On 13 January, 2018, the Bank of Italy published federal legislation (Legislative Decree 15 December 2017, n. 218) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	ITALY
Entry into Force	13 January 2018
National Transposition Law	Legislative Decree 15 December 2017, n. 218 http://www.gazzettaufficiale.it/eli/gu/2018/01/13/10/sg/pdf
Competent Authority	Bank of Italy http://www.bancaditalia.it/homepage/index.html
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.15.1 Italy: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

No information

Additional Notes	STATUS	In process of implementation
	EBA Comment: <i>intent to comply by 30.06.2018</i>	

4.15.2 Italy: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

No information

Additional Notes	STATUS	In process of implementation
	EBA comments: <i>Intent to comply. By 30.06.2018</i>	

4.15.3 Italy: Regulatory Technical Standards on authentication and communication

ITALY

Art. 5-bis (Confirmation of the availability of funds). -

2. The PSP may request confirmation as referred to in paragraph 1, when all the following conditions are satisfied:

c) before each confirmation request, the PSP authenticates with the ASPSP routing and communicates securely in accordance with the provisions of Article 98 (1)(d), of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission.

Art. 5 -ter (Provisions for access to payment accounts in the case of payment arrangement services). -

3. In order to ensure the exercise of the right of the payer to avail of the payment order provision service, the PSP of routing the account:

(a) communicate securely with payment service provision service providers in accordance with Article 98 (1)(b) d), of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission;

Art. 5 -quater (Provisions for access to information on payment accounts and their use in the case of information services on accounts). 2. The AISP:

(c) for each communication session, it is identified with the PSP or the ASPSP, by communicating with the latter and with the user in a secure manner, in accordance with Article 98 (1)(lit. d), of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission;

3. In relation to payment accounts, the PSP of routing the account:

(a) communicate securely with AISPs, in accordance with Article 98 (1)(lit. d), of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission;

Art. 10-bis (Authentication and security measures). -

1. In accordance with Article 98 of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission, PSPs shall apply SCA when the user:

a) access his online payment account;

b) has an electronic payment transaction;

c) perform any action, via a remote channel, which may involve a risk of payment fraud or other abuse.

3. In accordance with Article 98 of Directive (EU) 2015/2366 and the related RTS adopted by the European Commission, PSPs shall provide appropriate security measures to protect the confidentiality and integrity of security credentials personalized PSUs.

4.16 Latvia

On 4 July, 2018, the Latvian Financial and Capital Market Commission published legislation (Payment Services and Electronic Money Law) implementing the PSD2. The legislation enters into force on 18 July.

COUNTRY	LATVIA
Entry into Force	13 July 2018
National Transposition Law	Payment Services and Electronic Money Law https://likumi.lv/doc.php?id=206634

COUNTRY	LATVIA
Competent Authority	Financial and Capital Market Commission http://www.fktk.lv
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.16.1 Latvia: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Chapter XIV Operational and Security Risks and Authentication

Article 104.1 (1) Within the framework of an internal control system, the PSP is required to develop appropriate risk mitigation measures and control mechanisms for the management of operational and security risks related to payment services provided by it.

(2) Within the framework of an internal control system, the PSP establishes and maintains effective information system security incident management procedures, including procedures for the detection and classification of significant operational and security incidents.

(3) The PSP shall provide the Commission, by 31 January of each year, with an updated and comprehensive assessment of the operational and security risks associated with the payment services it provided in the previous year and of the adequacy of the exposure to those risks in response to those risks. Mitigation measures and control mechanisms implemented.

(4) The Commission issues regulatory provisions on the procedure for the determination, classification and reporting of operational and security incidents by PSPs.

(5) The Commission issues regulatory provisions on the procedure for the development, classification and provision of PSPs for operational and security risk assessments.

Additional Notes

Implemented by normative rules of the Financial and Capital Markets Commission (the Regulator) Nr. 158 "Informācijas sistēmu drošības noteikumi", October 5, 2018. The regulation implements the EBA Guidelines (2017) the existing document complemented.
<https://likumi.lv/ta/id/301983-informacijas-sistemu-drosibas-normativie-noteikumi>

STATUS

implemented

4.16.2 Latvia: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Chapter XIV Operational and Security Risks and Authentication

Article 104.2 (1) If a PSP detects a significant operational or information security incident, it shall immediately notify the Commission thereof.

(2) If a security incident affects or is likely to affect the financial interests of PSUs of a PSP, the PSP shall immediately inform its PSUs of the incident and of any measures that they may take to mitigate the adverse effects of this incident.

(3) The Commission, after receiving the report referred to in the first paragraph of this Article, shall immediately report a material incident to the EBA and the ECB. The Commission also informs other participants of the Latvian financial and capital market and the Information Technologies Security Incident Institution, the Institute of Mathematics and Computer Science of the University of Latvia, if necessary.

(4) If the Commission has received a report from the EBA or the ECB concerning a significant operational or information system security incident in another MS, it shall evaluate this report and, if necessary, inform the Information Technology Security incident prevention institution - the University of Latvia's Mathematical and Informatics institutions and PSPs that provide their services in Latvia, as well as take other measures to protect the security of the financial system.

Article 104.3. (1) A PSP shall submit to the Commission, twice a year, by 31 January and 31 July, statistical data on fraud and other unlawful activities during the preceding six months related to the use of means of payment in the previous half-year.

(2) The Commission issues regulatory provisions on the procedures by which PSPs submit statistics on fraud and illegal activities related to the use of means of payment.

Additional Notes	Has been implemented by Rules of the Regulator Nr. 157 “Normatīvie noteikumi par ziņošanu par būtiskiem maksājumu pakalpojumu incidentiem”, September 26, 2018. Implementing EBA Guidelines. https://likumi.lv/ta/id/301984-normativie-noteikumi-par-zinosanu-par-butiskiem-maksajumu-pakalpojumu-incidentiem	
	STATUS	Implemented

4.16.3 Latvia: Regulatory Technical Standards on authentication and communication

LATVIA		
<p>Article 81.1 (2) The PSP may require the approval referred to in the first paragraph if all of the following conditions are met:</p> <p>3) The PSP shall identify itself in the system of the PSP of the account and contact the PSP of the account before complying with the secure communication standards established by Commission delegated Regulation (EU) 2018/389 of 27 November 2017, which supplements Directive (2015/2366) of the European Parliament and of the Council with regard to the RTS for user authentication and uniform and secure open communication standards.</p> <p>Article 104.4 (6) PSPs shall comply with the requirements of the mutual security of communication and the strict authentication requirements set out in this Law, the regulatory enactments issued by the Commission, and Regulation 2018/389.</p> <p>(7) The PSP shall have the right to derogate from the requirements of this Article and to use the provisions of Regulation 2018/389.</p>		
ADDITIONAL NOTES	EBA RTS BINDING, IMPLEMENTED THROUGH THE LAW MAKSĀJUMU PAKALPOJUMU UN ELEKTRONISKĀS NAUDAS LIKUMS [PAYMENT SERVICES AND ELECTRONIC CURRENCY LAW]: HTTPS://LIKUMI.LV/DOC.PHP?ID=206634	
	STATUS	Implemented

4.17 Lithuania

On 1 August, 2018, the Bank of Lithuania published federal legislation (Payment law no. VIII-1370 amendment law) implementing the PSD2. The legislation enters into force on 1 August, 2018.

COUNTRY	LITHUANIA
Entry into Force	13 August 2018
National Transposition Law	Service Public Federal Finances https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/63e361e2488011e89197e1115e5dbeece
Competent Authority	Bank of Lithuania https://www.lb.lt/en/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.17.1 Lithuania: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)	
<p>Article 56 Operational and security risk management</p> <p>1. PSPs must establish risk mitigation measures and controls a system of mechanisms for managing PSPs operational and security risks. This system must have effective incident management procedures, including the identification and classification of major operational and security incidents.</p>	

2. PSPs must provide the supervisory authority with periodic updates and comprehensive operational and security risks associated with their payment services; and implement the assessment of the appropriateness of these risk mitigation measures and control mechanisms information. The supervisory authority determines the procedure and frequency of providing this information.
3. The supervisory authority, having regard to the findings of the EBA guidelines as referred to in Directive Article 95 (3) of Decision 2015/2366 determines the PSPs with regard to the preparation, implementation and implementation of security measures monitoring, including requirements for certification processes.

Additional Notes	Lithuania requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Lithuania requires PSPs to provide the Bank of Lithuania with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.
	Lithuania national law transposition: Article 56 Operational and security risk management 3. The supervisory authority, having regard to the findings of the EBA guidelines as referred to in Directive Article 95 (3) of Decision 2015/2366 determines the PSPs with regard to the preparation, implementation and implementation of security measures monitoring, including requirements for certification processes.
	Lithuania will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.17.2 Lithuania: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Article 57 Incident reports

1. In the event of a major operational or security incident, PSPs must immediately notify the supervisory authority thereof.
2. When an incident has or might affect the financial services of PSUs the PSP must immediately inform his PSUs about the incident and any measures they can take to reduce them negative consequences of the incident.
3. The supervisory authority shall, without delay, receive the notification referred to in paragraph 1 submit to the EBA and the ECB an appropriate comprehensive one information about the incident. The supervisory authority, having assessed the importance of the incident for other Lithuania The authorities of the Republic, inform them without delay of the incident.
4. The supervisory authority, upon receipt of a notification from the EBA or The ECB on a major operational or security event in another MS incident or receipt of a notice from the ECB concerning payment systems shall take all necessary measures to ensure immediate financial security system security.
5. The supervisory authority shall, having regard to the findings of the EBA the guidelines, as referred to in Article 96 (3) (a) of Directive 2015/2366, lay down requirements the PSPs for the operational and security operations referred to in paragraph 1 of this Article the classification of incidents and the procedure for reporting and reporting on such incidents.
6. PSPs must periodically submit statistical information to the supervisory authority data on fraud involving various payment instruments. Care the institution shall determine the content, procedure and frequency of the statistical information provided.
Care The authority shall provide aggregated data to the EBA and the ECB.

Additional Notes	Lithuania requires PSPs to notify the Bank of Lithuania without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Lithuania requires PSPs to periodically provide the Bank of Lithuania with statistical data on fraud related to different means of payment. Lithuania does not specify the periodicity of providing the information to the supervisory authorities.
	Lithuania national law transposition: Article 57 Incident reports 5. The supervisory authority shall, having regard to the findings of the EBA the guidelines, as referred to in Article 96 (3) (a) of Directive 2015/2366, lay down requirements the PSPs for the operational and security operations referred to in paragraph 1 of this Article the classification of incidents and the procedure for reporting and reporting on such incidents.
	Lithuania will apply the requirements established in the guideline on major incident reporting of the EBA.

4.17.3 Lithuania: Regulatory Technical Standards on authentication and communication

LITHUANIA

Article 2. The main concepts of this law

1. Open Link Interface - A publicly available technical interface for the relationship between ASPSPs, PISPs, AISP, other PSPs, payers and payees, prepared in accordance with a delegated act adopted by the European Commission as referred to in the Directive (EU) No 2015/2366, Article 98 (1) (d).

Article 58 Authentication

3. The PSP may waive the safer authentication procedure in a delegated act adopted by the European Commission as referred to in Article 4 of Directive (EU) No. 2015/2366 in Article 98 (1) (b).

7. The provisions of this Article shall be applied in the context of the delegated act adopted by the European Commission as referred to in Article 4 of Directive (EU) No. 2015/2366, Article 98 (1) (a), (b) and (c).

Article 59 The supervisory authority has the right to establish mandatory technical and operational requirements for an open communication interface

The Supervisory Authority has the right to determine the obligatory technical and / or technical aspects of the Open Link Interface operational requirements, as far as is not in conflict with the delegated act adopted by the European Commission, as referred to in Directive (EU) No. 2015/2366, Article 98 (1) (d), provided that these requirements are related to:

- 1) the safe and reliable operation of open communication interfaces;
- 2) the availability of open communication interfaces for PISPs and AISP;
- 3) Promotion of competition in the payment market.

4.18 Luxembourg

On 29 July, 2018, the Luxembourgian Financial Sector Supervisory Commission published federal legislation (Official Journal of the Grand Duchy of Luxembourg N ° 612 From 25 July 2018) implementing the PSD2. The legislation enters into force on 29 July, 2018.

COUNTRY	LUXEMBOURG
Entry into Force	29 July 2018
National Transposition Law	Official Journal of the Grand Duchy of Luxembourg N ° 612 From 25 July 2018 http://data.legilux.public.lu/file/eli-etat-leg-loi-2018-07-20-a612-jo-fr-pdf.pdf
Competent Authority	Financial Sector Supervisory Commission http://www.cssf.lu/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.18.1 Luxembourg: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Article 105-1. - Management of operational and security risks.

(1) PSPs shall establish a framework with appropriate mitigation measures and controls to manage the operational and security risks associated with the payment services they provide. This framework provides for PSPs to establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) PSPs shall provide the CSSF, at least annually, with an up-to-date and comprehensive assessment of the operational and security risks associated with the payment services they provide and information on the adequacy of the payment measures. Mitigation and control mechanisms put in place to deal with these risks.

Additional Notes

Luxembourg requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.

	Luxembourg requires PSPs to provide the Financial Sector Supervisory Commission with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.	
	STATUS	In process of implementation
	EBA comments²: <i>Intends to comply.</i> By such time as the necessary legislative or regulatory proceedings have been completed.	

4.18.2 Luxembourg: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Article 105-2. - The notification of incidents.

(1) In the event of an operational or major security incident, PSPs shall inform the CSSF without undue delay. Where the incident has or is likely to affect the financial interests of its PSUs, the PSP shall inform without undue delay its PSUs of the incident and all measures available that they can take to mitigate the damaging effects of the incident.

(2) Upon receipt of the notification referred to in paragraph (1), the CSSF shall without undue delay communicate the important details of the incident to the EBA and the ECB and, having assessed the relevance of the incident for other authorities concerned in Luxembourg, inform them accordingly. The CSSF cooperates with the EBA and the ECB to assess the relevance of the incident for other relevant authorities in Luxembourg, where appropriate, and the European Union. These are informed accordingly. On the basis of this notification, the CSSF or, as the case may be, the other authorities concerned shall take all the necessary measures to protect the immediate security of the financial system.

(3) PSPs must provide the CSSF, at least every year, with statistical data relating to fraud relating to the various means of payment. The CSSF provides this data in aggregate form to the EBA and the ECB.

Additional Notes	Luxembourg requires PSPs to notify the Financial Sector Supervisory Commission without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Luxembourg requires PSPs to provide the Financial Sector Supervisory Commission, once a year, with statistical data on fraud involving different means of payment.	
	STATUS	In process of implementation
	EBA comments²: <i>Intends to comply.</i> By such time as the necessary legislative or regulatory proceedings have been completed. The bill transposing the PSD2 in Luxembourg law is currently under discussion and the Luxembourg Parliament.	

4.18.3 Luxembourg: Regulatory Technical Standards on authentication and communication

LUXEMBOURG

Article 81-1. - Confirmation of the availability of funds.

Article 81-2. - The rules relating to access to the payment account in the case of PIS.

Article 81-3. - The rules on access to payment account data and the use of such data in the case of AIS.

Article 105-3. - Authentication.

4.19 Malta

On 1 January, 2018, the Central Bank of Malta published legislation (Directive No. 1: The Provision and Use of Payment Services and Chapter 376 Financial Institutions Act) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	MALTA
Entry into Force	13 January 2018
National Transposition Law	<p>Directive No. 1: The Provision and Use of Payment Services https://www.centralbankmalta.org/file.aspx?f=434 Chapter 376 Financial Institutions Act https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/Consultation/2018/Proposed%20Amendments%20to%20FIA.pdf</p>
Competent Authority	<p>Central Bank of Malta https://www.centralbankmalta.org Malta Financial Services Authority https://www.mfsa.com.mt/</p>
Supervision Authority	<p>Central Bank of Malta https://www.centralbankmalta.org</p>
Incident Reporting Authority	
Incident Reporting Channel	

4.19.1 Malta: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

11A. Management of operational and security risks.

(1) Payment institutions, electronic money institutions and AISP shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment institutions, electronic money institutions and AISP shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) Payment institutions, electronic money institutions and AISP shall provide to the CA on an annual basis, or at shorter intervals as may be determined by the CA, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

(3) The CA may issue, amend or revoke Financial Institutions Rules as may be required in order to better implement the provisions of this article.

Additional Notes	<p>Malta requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.</p> <p>Malta requires PSPs to provide the Malta Financial Services Authority with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.</p>
	<p>EBA comments: As at 12.03.2018, notification date. Please note that these Guidelines are the joint responsibility of both the MFSA and CBM and both have agreed to comply with these Guidelines.</p>
	<p>Malta will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.</p>

4.19.2 Malta: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

70. Incident reporting

(1) In the case of a major operational or security incident, PSPs shall, without undue delay, where Malta is the home MS, notify the Bank and the MFSA. PSPs shall use the procedures established by the EBA for notifying such incidents.

Where the incident has or may have an impact on the financial interests of its PSUs, the PSP shall, without undue delay, inform its PSUs of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

(2) Upon receipt of the notification referred to in Paragraph 70(1), the Bank shall, in collaboration with the MFSA, and without undue delay, provide the relevant details of the incident to the EBA and to the ECB. The Bank shall, in collaboration with the MFSA, assess the relevance of the incident to the relevant authorities in Malta, and notify any such authorities accordingly.

The Bank shall, in collaboration with the MFSA, cooperate with the EBA and the ECB for the purpose of assessing the relevance of the incident to other relevant European Union and national authorities in accordance with the obligations of the EBA and the ECB as laid down in Article 96(2) of Directive (EU) 2015/2366.

The Bank shall, on the basis of notifications received from the EBA and/or the ECB in accordance with their obligations as laid down in Article 96(2) of Directive (EU) 2015/2366, where appropriate and in collaboration with the MFSA, take all of the necessary measures to protect the immediate safety of the financial system.

(3) PSPs shall provide, on an annual basis, statistical data on fraud relating to different means of payment to the Bank. The Bank shall, in collaboration with the MFSA, provide the EBA and the ECB with such data in an aggregated format.

Additional Notes	Malta requires PSPs to notify the Central Bank of Malta and Malta Financial Services Authority without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Malta requires PSPs to provide the Central Bank of Malta, once a year, with statistical data on fraud involving different means of payment.
	EBA comments⁴: As at 14.02.2018, notification date.
	Malta will comply with the guideline on major incident reporting issued by the EBA.

4.19.3 Malta: Regulatory Technical Standards on authentication and communication

MALTA

71. Authentication

(1) PSPs shall apply SCA in line with the provisions established in the Financial Institutions Rules on Security of Internet Payments of Credit, Payment and Electronic Money Institutions (FIR/04/2015), where the payer:

- (a) accesses its payment account online;
- (b) initiates an electronic payment transaction, including card transactions;
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

Provisions established in the Financial Institutions Rules on Security of Internet Payments of Credit, Payment and Electronic Money Institutions (FIR/04/2015) with regards to SCA will be superseded by the RTS referred to in Article 98 of Directive (EU) 2015/2366, 18 months after the date of entry into force of such RTS.

4.20 Netherlands

NETHERLANDS			
STATUS OF THE TRANSPOSITION	In process of implementation	Enter into force	Beginning 2019
NATIONAL LAW TRANSPOSED	Implementatiewet herziene richtlijn betaaldiensten https://zoek.officielebekendmakingen.nl/dossier/34813/kst-34813-A?resultIndex=13&sorttype=1&sortorder=4		

NETHERLANDS	
COMPETENT AUTHORITY	De Nederlandsche Bank (DNB) https://www.dnb.nl/
SUPERVISION AUTHORITY	DNB, Dutch Authority for the Financial Markets (AFM), https://www.afm.nl/ , The Netherlands Authority for Consumers and Markets (ACM), https://www.acm.nl/
INCIDENT REPORTING AUTHORITY	DNB

4.20.1 Netherlands: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)		
No information		
COMPETENT AUTHORITY		
ASSESSMENT (DIFFERENCES WITH PSD2)	n/a	
GUIDELINES ADAPTATION	STATUS	In process of implementation
	n/a	
	DIFFERENCES WITH EBA	n/a
	n/a	

4.20.2 Netherlands: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)		
No information		
COMPETENT AUTHORITY		
ASSESSMENT (DIFFERENCES WITH PSD2)	n/a	
GUIDELINES ADAPTATION	STATUS	In process of implementation
	n/a	
	DIFFERENCES WITH EBA	n/a
	n/a	
REPORTING CHANNEL	n/a	

4.20.3 Netherlands: Regulatory Technical Standards on authentication and communication

NETHERLANDS	
No information	

4.21 Poland

On 5 June, 2018, the Polish Financial Supervision Authority published legislation (Act on payment services) implementing the PSD2. The legislation enters into force on 31 December, 2018.

COUNTRY	MALTA
Entry into Force	31 December 2018
National Transposition Law	Act on payment services http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001075/O/D20181075.pdf
Competent Authority	Polish Financial Supervision Authority https://www.knf.gov.pl/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.21.1 Poland: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

CHAPTER IIA Security of the provision of payment services

Art. 32f. 1. The supplier, as part of the risk management system, takes measures to limit the risk and introduces control mechanisms for managing operational risk and security risk in the provision of payment services, in particular by:

- 1) maintaining an effective incident management procedure, including for the detection and classification of serious incidents operational incidents and incidents related to security, including ICT;
 - 2) ongoing assessment and updating of procedures in the area of operational risk management and infringement risk security, including ICT security, as well as ongoing assessment of restrictive measures risk and control mechanisms.
2. The supplier submits to the KNF or another competent authority annually by 31 January of the following year supervisory body, annual information on the assessment and updating of procedures in the area of operational risk management and the risk of breach of security, as well as risk mitigation measures and mechanisms controls referred to in paragraph 1 point 2.

Additional Notes	Poland requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Poland requires PSPs to provide the Polish Financial Supervision Authority with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or before January 31 of the following year.
	Poland has notified its adaptation of March 12, 2018, but no information has been found on website of its competent authority.
	Poland will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.21.2 Poland: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

CHAPTER IIA Security of the provision of payment services

Article 32g 1. The supplier shall immediately forward the information to the Polish Financial Supervision Authority or to another competent supervisory authority about a serious operational incident or security incident, including of a tele-informatic nature.

2. If the incident referred to in paragraph 1, has or may affect the financial interests of users, the provider shall without undue delay notify the incident of users using the services of that provider and informs them of available measures that they can take to limit the negative effects of the incident.
 3. The information referred to in paragraph 1, the Polish Financial Supervision Authority or other competent supervisory authority shall immediately transmit to EBA and the ECB, and if the incident is relevant to the supervisory authority of another Member State - also this authority.
 4. If the Polish Financial Supervision Authority or other competent supervisory authority receives information from the EBA or the ECB about the incident it has importance for the domestic financial market, immediately takes the necessary steps to protect security financial system.
- Art. 32h. 1. The Supplier annually, by 31 January of the following year, provides the Polish Financial Supervision Authority or other competent supervisory authority with annual data on fraud related to payment services performed, taking into account the different ways of providing payment services.
2. Based on the data received in accordance with paragraph 1, the PFSA and other competent supervisory authority shall, by 30 June of a given year, provide EBA and the ECB with aggregated data on fraud related to payment services performed, taking into account the different ways of providing payment services.

Additional Notes	Poland requires PSPs to notify the Polish Financial Supervision Authority without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Poland requires PSPs to provide the Polish Financial Supervision Authority, annually before 31 January of the following year, statistical data on fraud related to payment services. The Polish Financial Supervision Authority will provide the EBA and ECA with the statistical data received from the PSPs, annually before June 30 of the same year that they have received the statistical data.
	Poland has notified its adaptation of February 19, 2018, but no information has been found on website of its competent authority.
	Poland will comply with the guideline on major incident reporting issued by the EBA.

4.21.3 Poland: Regulatory Technical Standards on authentication and communication

POLAND

Article 49a.

1. The account provider, at the request of the provider issuing payment instruments based on a payment card, immediately confirms the availability on the payment account of the payer of the amount necessary to perform the payment transaction based on this card, if:
 - 3) the supplier authenticates himself to the account provider before submitting the application referred to in para. 1, and in a safe manner communicates with this supplier in accordance with the requirements set out in Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive of the European Parliament and of the Council (EU) 2015/2366 with regard to RTS aspects of SCA and common and secure open communication standards (OJ L 69 of 13/03/2018, p. 23).

Article 59r.

3. The provider providing the service of initiating a payment transaction:
 - 4) in the case of initiating payments - is obliged to identify himself / herself against the account provider and communicate with the account provider, payer and recipient in a secure manner, in accordance with the requirements set out in Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to RTS for SCA and common and secure open communication standards;
4. The account provider:
 - 1) is obliged to communicate with providers providing the service of initiating a payment transaction in a secure manner, in accordance with the requirements set out in Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive of the European Parliament and of the Council (EU) 2015/2366 with regard to RTS for SCA and common and secure open communication standards;

Article 59s.

2. Provider providing a service for access to account information:
 - 3) in the case of a communication session - is obliged to identify himself / herself against the account provider to the user and communicate with the account provider and user in a secure manner, in accordance with the requirements set out in Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive of the European Parliament and of the Council (EU) 2015/2366 with regard to RTS regarding SCA and common and secure open communication standards;
3. The account provider:
 - 1) is obliged to communicate with providers providing access to account information in a secure manner, in accordance with the requirements set out in Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive of the

POLAND

European Parliament and of the Council (EU) 2015/2366 with regard to RTS regarding SCA and common and secure open communication standards;

4.22 Portugal

PORTUGAL			
STATUS OF THE TRANSPOSITION	Transposed	ENTER INTO FORCE	13 November 2018
NATIONAL LAW TRANSPOSED	The national law of the PSD2 (English): Decree-Law No. 91/2018, of November 12 Decreto-Lei n.º 91/2018, de 12 de novembro https://www.bportugal.pt/sites/default/files/anexos/legislacoes/335415275_2.docx.pdf		
COMPETENT AUTHORITY	Bank of Portugal https://www.bportugal.pt/		
SUPERVISION AUTHORITY			
INCIDENT REPORTING AUTHORITY			

4.22.1 Portugal: Guidelines on the Security Measures

ARTICLE 95 MANAGEMENT OF OPERATIONAL AND SECURITY RISKS	
PSD2	<p>1. MS shall ensure that PSPs establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, PSPs shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.</p> <p>2. MS shall ensure that PSPs provide to the CA on an annual basis, or at shorter intervals as determined by the CA, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.</p>
TRANSPOSITION	<p>Article 70 - Operational and safety risk management</p> <p>1. Payment service providers shall establish a framework with adequate mitigation measures and control mechanisms to manage operational and safety risks related to the payment services they provide.</p> <p>2 - As part of the framework referred to in the preceding paragraph, payment service providers establish and maintain effective incident management procedures, including for the detection and classification of severe operational and security incidents.</p> <p>3 - Payment service providers shall provide Banco de Portugal with an annual or shorter periodicity, a thorough and up-to-date assessment of the operational and security risks related to the payment services provided by them, as well as the adequacy the risk mitigation measures and the control mechanisms applied in response to those risks.</p> <p>4 - The Bank of Portugal establishes the regulatory rules regarding the definition, application and monitoring of the security measures mentioned in this article.</p>
Additional notes	<p>Portugal requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.</p> <p>Portugal requires PSPs to provide the Banco of Portugal with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.</p>

4.22.2 Portugal: Guidelines on Major Incident Reporting

GUIDELINES ON SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS UNDER PSD2 ¹³	NATIONAL TRANSPOSITION	
	STATUS	In process of implementation
ARTICLE 96 INCIDENT REPORTING		
PSD2	<p>1. <u>In the case of a major operational or security incident, PSPs shall, without undue delay, notify the CA in the home MS of the PSP.</u></p> <p>Where the incident has or may have an impact on the financial interests of its PSUs, the PSP shall, without undue delay, inform its PSUs of the incident and of all measures that they can take to mitigate the adverse effects of the incident.</p> <p>2. Upon receipt of the notification referred to in paragraph 1, <u>the CA of the home MS shall, without undue delay, provide the relevant details of the incident to EBA and to the ECB.</u> That CA shall, after assessing the relevance of the incident to relevant authorities of that MS, notify them accordingly.</p> <p>EBA and the ECB shall, in cooperation with the CA of the home MS, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system.</p> <p>On the basis of that notification, the CAs shall, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.</p> <p>6. MSs shall ensure that PSPs <u>provide</u>, at least on an annual basis, <u>statistical data on fraud relating to different means of payment to their CAs.</u> Those CAs shall provide EBA and the ECB with such data in an aggregated form.</p>	
TRANSPOSITION	<p>Article 71 - Reporting of incidents</p> <p>1 - In the case of a severe operational or security incident, payment service providers based in Portugal:</p> <p>a) Notify Banco de Portugal without delay, without prejudice to other notifications which are due under national or European legislation applicable to payment service providers and to electronic money issuers, such as those applicable to the protection of individuals with regard to the processing of personal data; and</p> <p>b) if the incident has or is likely to have an impact on the financial interests of its payment service users, it shall inform them without delay of the incident and of all steps they can take to mitigate its adverse effects.</p> <p>2 - Banco de Portugal establishes the regulatory rules regarding the classification by payment service providers of the incidents of a severe nature referred to in paragraph 1 (a) of this article and the content, format, including standardized communication models, and procedures for reporting such incidents by payment service providers.</p> <p>3. Upon receipt of the communication referred to in paragraph 1 (a) of this Article, Banco de Portugal shall:</p> <p>(a) provide the European Banking Authority and the European Central Bank without delay with the relevant details of the incident ; and (b) notifies the relevant national authorities, after assessing the relevance of the incident to them.</p> <p>4. The Bank of Portugal shall cooperate with the European Banking Authority and the European Central Bank in assessing the relevance of the incident to other relevant authorities of other Member States and the Union, taking into account in particular the notifications received by the European Central Bank in respect of other matters relevant information.</p> <p>5 On the basis of the notifications referred to in this article, Banco de Portugal shall, as appropriate, take all necessary measures to protect the immediate security of the financial system.</p>	
Additional notes	<p>Portugal requires PSPs to notify the Banco de Portugal without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.</p> <p>Portugal requires PSPs to provide the Banco de Portugal, once a year, with statistical data on fraud involving different means of payment.</p>	

4.22.3 Portugal: Regulatory Technical Standards on authentication and communication

¹³ https://www.eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_EN.pdf/c63cfcbf-7412-4cfb-8e07-47a05d016417

ARTICLE 98 REGULATORY TECHNICAL STANDARDS ON AUTHENTICATION AND COMMUNICATION	
PSD2	<p>1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft RTS addressed to PSPs as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:</p> <p>(a) the requirements of the SCA referred to in Article 97(1) and (2);</p> <p>(b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article;</p> <p>(c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the PSUs' personalised security credentials; and</p> <p>(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between ASPSPs, PISPs, AISP, payers, payees and other PSPs.</p>
TRANSPOSITION	<p>Article 105 Confirmation of the availability of funds</p> <p>6. Authentication and communication between the payment service provider issuing card-based payment instruments and the payment service provider who manages the account referred to in paragraph 2 (c) shall be subject to the provisions of the delegated act of the European Commission adopting the regulatory technical standards, pursuant to Article 98 (1) of Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015.</p> <p>Article 106 Access to payment account in case of payment initiation services</p> <p>6. The identification and communication between the payment service provider and the payment service provider who manages the account referred to in paragraph 3 (d) and paragraph (a) 4 shall be subject to the provisions of the delegated act of the European Commission adopting regulatory technical standards pursuant to Article 98 (1) of Directive 2015/2366 of the European Parliament and of the Council, of November 25, 2015.</p> <p>Article 107 Access to information on the payment account and its use in the case of account information services</p> <p>5 - Identification and communication between the account information service provider and the payment service provider who manages the account referred to in paragraph 2 (c) and paragraph 2 (a) 3 shall be subject to the provisions of the delegated act of the European Commission adopting regulatory technical standards, pursuant to Article 98 (1) of Directive 2015/2366 of the European Parliament and of the Council of November 25, 2015.</p>
Additional notes	<p>Article 98 of the PSD2 has been integrated into several articles of the national payment service law of Portugal. Portugal will directly apply the commission delegated regulation (EU) 2018/389, RTS for SCA and common and secure open standards of communication.</p>

4.23 Romania

COUNTRY	ROMANIA
Entry into Force	26 March 2018
National Transposition Law	<p>Draft legislative act Emergency Ordinance on Payment Services</p> <p>http://www.anpc.gov.ro/galerie/file/proiecte_acte/2018/oug_serviciile_de_plata.pdf</p>
Competent Authority	<p>National Bank Romania</p> <p>http://www.bnr.ro/Home.aspx</p>
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	

4.23.1 Romania: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

SECTION 1 Managing Operational and Security Risks and Incident Reporting

Art. 218. - 1. Payment service providers shall establish a framework of appropriate measures and control mechanisms to manage the operational and security risks related to the payment services they provide. As part of this framework, payment service providers shall establish, update and implement effective incident management procedures, including the identification and classification of major operational and security incidents.

(2) The persons provided in art. 223 par. (1) Provide annually to the National Bank of Romania, in the form requested by it, an updated and comprehensive assessment of the operational and security risks related to the payment services it provides and on the adequacy of the mitigation measures and mechanisms control implemented in response to these risks.

(3) The National Bank of Romania may modify the transmission frequency of the assessment provided for in paragraph (2) by payment service providers in accordance with its rules.

(4) In order to prevent and mitigate the operational and security risks associated with the payment services provided by the persons referred to in art. 223 par. (1), the National Bank of Romania may cooperate and 53 participate in the exchange of information with other competent authorities, the European Central Bank and the European Banking Authority and, where appropriate, the European Network and Information Security Agency.

Additional Notes

Romania requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.
Romania requires PSPs to provide the National Bank of Romania with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.

4.23.2 Romania: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Art. 219 - (1) The payment service providers referred to in art. 223 par. (1) Romanian legal persons which provide payment services on Romanian territory as well as on the territory of other Member States through branches, agents or directly notify to the National Bank of Romania any major operational or security incident without undue delay and in the form requested by the National Bank of Romania.

2. Where the incident has or may have an impact on the financial interests of the payment service users of the payment service provider, the payment service provider shall without undue delay inform the relevant users of the incident and of all measures on which users can take to mitigate its negative effects.

(3) Upon receipt of the notification referred to in paragraph (1), the National Bank of Romania shall, without undue delay, forward the relevant details of the incident to the European Banking Authority and to the European Central Bank. After assessing the relevance of the incident to other national authorities in Romania, the National Bank of Romania shall notify them accordingly.

4. Payment service providers in a Member State which provide payment services in Romania through branches, agents or directly notify any major operational or security incident to the competent authority of the home Member State.

5. On the basis of the notification received from the European Central Bank and / or the European Banking Authority of an incident reported to them by the competent authority of the payment service provider's home Member State which registered the payment incident, the Bank The National Bank of Romania shall, where appropriate, take all necessary measures to protect the immediate security of the financial system.

6. Paying service providers shall provide, at least annually, statistical data on frauds relating to different means of payment. The National Bank of Romania shall transmit this aggregate data to the European Banking Authority and the European Central Bank.

(7) In the exercise of the duties stipulated in paragraph (5), the National Bank of Romania may cooperate with other relevant national authorities or other Member States.

Additional Notes

Romania requires PSPs to notify the National Bank of Romania without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.
Romania requires PSPs to provide the National Bank of Romania, once a year, with statistical data on fraud involving different means of payment.

STATUS

In process of implementation

4.23.3 Romania: Regulatory Technical Standards on authentication and communication

ROMANIA

No information

4.24 Slovakia

On 11 March, 2018, the National Bank of Slovakia published federal legislation (Draft law 624/2017) implementing the PSD2. The legislation enters into force on 13 January, 2018.

COUNTRY	SLOVAKIA
Entry into Force	13 January 2018
National Transposition Law	Draft law 624/2017 https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=441236
Competent Authority	National Bank of Slovakia https://nbs.sk/sk/titulna-stranka
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting mail channel: National bank of Slovakia ccp@nbs.sk

4.24.1 Slovakia: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Section 28c

(1) The PSP shall determine the framework with appropriate measures to mitigate operational risk and security risk and a control mechanism to manage those risks associated with the provision of payment services. As part of this framework, the PSP shall introduce and apply effective incident management procedures, including the identification and breakdown of major operational incidents and security incidents ("incident").

(2) The PSP shall provide at least annually to the National Bank of Slovakia an updated and comprehensive assessment of operational risk and security risk management related to the provision of payment services as well as the adequacy of measures to mitigate such risks and established control mechanisms to respond to such risks.

(3) The National Bank of Slovakia cooperates with the European Supervisory Authority (EBA), the ECB and, where appropriate, with the ENISA for Exchange of Information on Operational Risk and Security Risk Related to Payment Services.

Additional Notes	Slovakia requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Slovakia requires PSPs to provide the National Bank of Slovakia with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.	
	STATUS	In process of implementation

4.24.2 Slovakia: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Section 28d

- (1) In the event of an incident, the PSP shall inform the National Bank of Slovakia without delay. The PSP, in the event of an incident affecting the financial interests of its PSUs, shall promptly inform its PSUs of the incident and of any action it may take to mitigate the adverse effects of the incident.
- (2) The National Bank of Slovakia, upon receipt of the notification pursuant to paragraph 1, shall promptly provide information on the incident to the European Supervisory Authority (EBA) and the ECB. The National Bank of Slovakia, following the assessment of this incident by the European Supervisory Authority (EBA) and the ECB, informs the National Security Authority or other competent national authorities in the Slovak Republic that they will take the necessary measures to protect the security of the financial system.
- (3) The PSP shall provide at least annually to the National Bank of Slovakia statistical data on fraud related to payment transactions. In aggregated form, the National Bank of Slovakia shall provide such data to the European Supervisory Authority (EBA) and the ECB.

Additional Notes	<p>Slovakia requires PSPs to notify the National Bank of Slovakia without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.</p> <p>Slovakia requires PSPs to provide the National Bank of Slovakia, once a year, with statistical data on fraud involving different means of payment.</p> <p>National Bank of Slovakia comments: The reporting person (i.e. the payment service provider of the payer) may submit a notification using the special means of communication of the National Bank of Slovakia. The special means of communication are separated from the normal means of communication of the National Bank of Slovakia, they are secure, and they guarantee the confidentiality of the data and are established in such a way as to prevent the access of unauthorized persons.</p> <p>Notification of a major incident is a notification of a single event or a series of related events not foreseen by the notifying party (payment service provider) that have, or are likely to have, adverse effects on the integrity, availability, confidentiality, reliability and / or continuity of payment services.</p> <p>As part of the process of reporting a person to manage incidents under Section 28c 1 of the Act on Payment Services is the identification and classification of operational incidents and security incidents ("incident").</p> <p><u>The reporting person should assess the incident according to the criteria and related indicators mentioned in the EBA Guideline.</u> If the reporting entity delegates notification of serious incidents to a third party, it should notify the National Bank of Slovakia and ensure the conditions set out in EBA Guideline.</p>
------------------	---

4.24.3 Slovakia: Regulatory Technical Standards on authentication and communication

SLOVAKIA

§ 3a Rights and obligations in the provision of PISs

- (3) A PISPs is required
- (d) Identify each other and initiate a payment transaction with a PSP in a secure manner, in accordance with the special regulation on the issuance of a RTS issued under a separate regulation, when providing a PIS to a PSP maintaining a payment account.
- (5) The PSP keeping a payment account is required
- (a) to communicate in a secure manner with the PAO in accordance with a special regulation on the issuance of a RTS issued under a separate regulation 15a) and immediately upon receipt of the payment order from the PIC to provide or disclose all information on the initiation of a payment transaction any information relating to its execution which is accessible to the PSP maintaining the payment account,

§ 3b Rights and Obligations to PISPs

- (2) The PSP shall be obliged to (d) be identified in every communication with the PSP who maintains the payment account and communicate with him as well as with the PSUs in a secure manner, in accordance with the special regulation on the issuance of the RTS issued on the basis of a separate regulation.)
- (4) The PSP cannot require the PSU to accept sensitive payment data related to the payment account and to use or store the data for purposes other than the execution of a payment service information service explicitly requested by the PSU or to such data access in accordance with a special regulation on the issuance of a RTS issued under a separate regulation.)
- (5) The PSP keeping a payment account is required
- (a) to communicate in a secure manner with the PSP of the payment account in accordance with the special regulation on the issuance of a RTS issued under a separate regulation); and

§ 3c SCA of the PSU

- (6) The PSP that maintains the payment account, the PAO and the AISP shall proceed with the SCA of the PSU pursuant to paragraphs 1 to 5 in accordance with a special regulation on the issue of a RTS issued under a separate regulation.).

SLOVAKIA

§ 28b

- (2) The PSP may request the sending of a confirmation pursuant to paragraph 1, if
(c) the PSP authenticates the PSP with each payment request and maintains the payment account and safely communicates with it in accordance with a separate regulation on the issue of a RTS issued under a separate regulation.

4.25 Slovenia

In 2018, the Bank of Slovenia published federal legislation (Law on payment services, services for issuing electronic money and payment systems) implementing the PSD2. The legislation enters into force on 22 February, 2018.

COUNTRY	SLOVENIA
Entry into Force	22 February 2018
National Transposition Law	Law on payment services, services for issuing electronic money and payment systems https://www.uradni-list.si/_pdf/2018/Ur/u2018007.pdf
Competent Authority	Bank of Slovenia https://www.bsi.si/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting email channel: Bank of Slovenia PSD2.porocanje@bsi.si

4.25.1 Slovenia: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Article 151 (management of operational and security risks)

(1) PSPs shall establish a framework with the appropriate ones measures to reduce risks and control mechanisms to manage operational and security risks associated with the payment services they provide. PSPs as part of this framework, establish and maintain effective procedures for incident management, including for detection and ranking major operational and security incidents.

(2) PSPs of the Bank of Slovenia once annually or at shorter intervals, as determined by the Bank of Slovenia, submit an updated and comprehensive assessment of the operational and security risks associated with the payment services they provide, and the assessment of the adequacy of risk mitigation measures and control mechanisms implemented in response to these risks.

Additional Notes	Slovenia requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Slovenia requires PSPs to provide the Bank of Slovenia with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.
	Official Gazette of the Republic of Slovenia comments²: 469. Decision on the application of the Guidelines on security measures for operational and security risks in payment services under Directive (EU) 2015/2366 (PSD2), page 1699. <u>Article 2 (Content of the decision and scope of the guidelines)</u> (1) By this Decision, the Bank of Slovenia shall determine the application of the guidelines for: 1. banks and savings banks which, in accordance with the ZBan-2, obtained the authorization to provide banking services in the Republic of Slovenia, 2. payment institutions and payment institutions with a waiver that have been granted authorization to provide payment services in accordance with ZPlaSSIED as a payment

	<p>institution or a payment institution with a waiver in the Republic of Slovenia, and an electronic money and electronic money issuing company with a suspension pursuant to ZPlaSSIED, have been granted an authorization to provide electronic money issuing services in the Republic of Slovenia, and</p> <p>3. The Bank of Slovenia, in accordance with ZPlaSSIED, ZBan-2 and Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ L 176 of 27 June 2013, page 1, hereinafter: Regulation (EU) No 575/2013) exercises the powers and tasks of supervision over entities 1 and 2 in the role of the competent authority.</p> <p>(2) The entities referred to in points 1 and 2 of the first paragraph of this Article shall fully comply with the provisions of the guidelines in so far as they are addressed to the payment service providers.</p> <p>(3) In carrying out the tasks and powers of supervision in accordance with ZPlaSSIED, ZBan-2 and Regulation (EU) no. 575/2013 and fully respects the provisions of the Guidelines in so far as they relate to the exercise of the tasks and powers of the competent authority.</p> <p>Slovenia will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.</p>
--	---

4.25.2 Slovenia: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Article 152 (incident reports)

- (1) PSPs established in the Republic of Slovenia shall notify the Bank of Slovenia of any major operational or security incidents without undue delay.
- (2) Where the incident affects or may affect financial interests its PSUs, the PSP the service informs its users without undue delay payment services on the incident and on any available measures that they can take them in order to reduce the negative effects of the incident.
- (3) The Bank of Slovenia shall, upon receipt of the notification referred to in the first paragraph of this Article without undue delay to the European Commission the Banking Authority and the ECB details of the incident. When the Bank of Slovenia assesses the incident for other relevant authorities of the Republic of Slovenia, it shall inform those authorities accordingly.
- (4) The Bank of Slovenia shall cooperate with the EBA and the ECB when assessing relevance incident for other relevant Union bodies and home authorities.
- (5) Where the EBA and the ECB the Bank shall inform the Bank of Slovenia of a major operational or financial institution security incident, the Bank of Slovenia, on the basis of this notice, where appropriate, take all necessary measures for ensuring the direct security of the financial system.
- (6) PSPs established in the Republic Slovenia must submit to the Bank of Slovenia at least once a year fraud and fraud related statistics payment methods. Bank of Slovenia this information in aggregate form the EBA and the ECB bank.

Additional Notes	<p>Slovenia requires PSPs to notify the Bank of Slovenia without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.</p> <p>Slovenia requires PSPs to provide the Bank of Slovenia, at least once a year, with statistical data on fraud involving different means of payment.</p>
	<p>Official Gazette of the Republic of Slovenia comments⁴: 470. Decision on the application of the Guidelines on Reporting Major Incidents in accordance with Directive (EU) 2015/2366 (PSD2), page 1700.</p> <p>Article 2 (Content of the decision and scope of the guidelines)</p> <p>(1) By this Decision, the Bank of Slovenia shall determine the application of the guidelines for:</p> <ol style="list-style-type: none"> 1. banks and savings banks which, in accordance with the ZBan-2, obtained the authorization to provide banking services in the Republic of Slovenia, 2. payment institutions and payment institutions with a waiver that have been granted authorization to provide payment services in accordance with ZPlaSSIED as a payment institution or a payment institution with a waiver in the Republic of Slovenia, and an electronic money and electronic money issuing company with a suspension pursuant to ZPlaSSIED, have been granted an authorization to provide electronic money issuing services in the Republic of Slovenia, and 3. The Bank of Slovenia, in accordance with ZPlaSSIED, ZBan-2 and Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ L 176

	<p>of 27 June 2013, page 1, hereinafter: Regulation (EU) No 575/2013) exercises the powers and tasks of supervision over entities 1 and 2 in the role of the competent authority.</p> <p>(2) The entities referred to in points 1 and 2 of the first paragraph of this Article shall fully comply with the provisions of the guidelines in so far as they are addressed to the payment service providers.</p> <p>(3) In carrying out the tasks and powers of supervision in accordance with ZPlaSSIED, ZBan-2 and Regulation (EU) no. 575/2013 takes full account of the provisions of the Guidelines in so far as they relate to the exercise of the tasks and powers of the competent authority.</p>
	Slovenia will comply with the guideline on major incident reporting issued by the EBA.

4.25.3 Slovenia: Regulatory Technical Standards on authentication and communication

SLOVENIA

Article 117 (confirmation of the availability of funds)

(2) A PSP issuing card payment instruments may request the certificate referred to in the preceding paragraph when the following conditions are met:

3. Before each request for confirmation, the PSP issuing card payment instruments shall demonstrate its identity with the PSP that administers the account and in accordance with the RTS adopted by the European Commission in accordance with the fourth paragraph of Article 98 Of Directive 2015/2366 / EU, communicates securely with the PSP that administers the account.

Article 118 (rules on access to a payment account for payment order services)

(3) Service provider of ordering payments;

4. demonstrate, in each payment order, his identity with the PSP keeping the account of the payer and in accordance with the RTS adopted by the European Commission in accordance with Article 98 (4) of Directive 2015/2366 / EU in a safe manner communicates with the PSP that administers the account, and with the payer and the payee,

Article 119 (rules on access to information on payment accounts for services in providing information on accounts and on the use of this information)

(2) Provider of information provision services;

3. demonstrate, at each communication, its identity with the PSP keeping the account of the PSU and in accordance with the RTS adopted by the European Commission in accordance with the fourth paragraph of Article 98 of Directive 2015/2366 / EU, the method communicates with the PSP that administers the account and with the PSU

(3) The PSP that keeps the account in relation to payment accounts:

1. securely communicates with providers of information provision services in accordance with RTS adopted by the European Commission in accordance with the fourth paragraph of Article 98 of Directive 2015/2366 / EU,

Article 332 (prohibition of abuse of non-compliance with the RTS referred to in Article 98 of Directive 2015/2366 / EU for blocking or hindering the use of payment orders and invoicing information services)

Individual PSPs that keep accounts in accordance with Article 21 of this Act until they comply with the RTS adopted by the European Commission in accordance with the fourth paragraph of Article 98 of Directive 2015/2366 / EU (hereinafter referred to as "technical standards") shall not abuse the incompatibility of its operation with technical standards for blocking or obstructing the use of payment orders in accordance with Article 118 of this Act and the provision of information on accounts in accordance with Article 119 of this Act for the accounts they keep.

4.26 Spain

In process of implementation

COUNTRY	SPAIN
Entry into Force	25 November
National Transposition Law	Royal Decree-Law 19/2018, of November 23 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16036
Competent Authority	Bank of Spain https://www.bde.es
Supervision Authority	

COUNTRY	SPAIN
Incident Reporting Authority	
Incident Reporting Channel	

4.26.1 Spain: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

CHAPTER V Operational and security risks

Article 61. Management of operational and security risks.

1. The PSPs will establish a framework, in accordance with the provisions of the Bank of Spain, with palliative measures and adequate control mechanisms to manage operational and security risks related to the payment services they provide. As part of this framework, PSPs will establish and maintain effective incident management procedures, in particular for the detection and classification of serious operational and security incidents.

2. The PSPs will provide the Bank of Spain, with the periodicity and form that it determines, with an up-to-date and complete evaluation of the operational and security risks associated with the payment services they provide and the adequacy of the mitigating measures and mechanisms of control applied in response to such risks.

Additional Notes	Spain requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Spain requires PSPs to provide the Bank of Spain with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.	
	STATUS	In process of implementation

4.26.2 Spain: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

CHAPTER V Operational and security risks

Article 62. Notification of incidents.

1. PSPs will notify the Bank of Spain, immediately and in the manner it determines, of serious operational or security incidents. If the security incident affects or could affect the financial interests of the PSUs, the PSP will inform them without undue delay of the incident and of all available mitigating measures that they may adopt to mitigate the adverse consequences of the incident.

2. The Bank of Spain will provide without undue delay the pertinent details of the incident to the European Banking Authority (ABE) and the European Central Bank (ECB). The Bank of Spain, after evaluating the importance of the incident for other national authorities, will inform them as appropriate.

The ABE and the ECB, in collaboration with the Bank of Spain, will assess the importance of the incident for other relevant Union and national authorities and notify them of the incident as appropriate.

3. When the Bank of Spain is notified by another competent authority in the manner indicated in the previous section, it will take, where appropriate, the necessary measures to protect the immediate security of the financial system.

4. The PSPs will provide the Bank of Spain, in the manner and with the periodicity that it determines, at least once a year, statistical data on fraud related to different means of payment. This information will be provided by the Bank of Spain in an aggregate form to the ABE and the ECB.

Additional Notes	Spain requires PSPs to notify the Bank of Spain without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence. Spain requires PSPs to provide the Bank of Spain, once a year, with statistical data on fraud involving different means of payment.	
	STATUS	In process of implementation

4.26.3 Spain: Regulatory Technical Standards on authentication and communication

SPAIN

No information

4.27 Sweden

On April 23, 2018, the Swedish Financial Supervisory Authority published federal legislation (Finansinspektionen's regulations regarding PSP) implementing the PSD2. The legislation enters into force on May 01, 2018.

COUNTRY	SWEDEN
Entry into Force	01 May 2018
National Transposition Law	Service Public Federal Finances https://www.fi.se/contentassets/72e226a0abe14cecb44443fedd2f12c1/fs1804.pdf
Competent Authority	Financial Supervisory Authority https://www.fi.se/sv/
Supervision Authority	
Incident Reporting Authority	
Incident Reporting Channel	Reporting web channel: Finansinspektionen? https://reportingportal.finansinspektionen.se/

4.27.1 Sweden: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Chapter 5 Systems of operational risks and security risks

Section 1 The system that a PSP must have in accordance with Chapter 5b. Section 1 of the Payment Services Act (2010: 751) shall be adapted to the supplier's operations and consist of a framework of documented measures that manage or reduce the risk of operational incidents or security incidents. Within the framework of the system, the supplier must at least

1. Define and assign the responsibilities that the provider considers necessary to carry out the security measures,
2. Determine processes, routines and systems to identify, measure, monitor and manage the risks associated with the provider's payment service business,
3. Make a risk assessment of payment services and provide a description of the security measures that will protect PSUs against the identified risks, including fraud and illegal use of sensitive data and personal data,
4. Have an internal level-based model for managing and controlling risks in the payment service business,
5. Provide a description of how the supplier ensures that the operational risks and security risks are handled when it instructs someone else to perform a portion of the payment service business,
6. Establish a risk appetite for payment service operations and inventory, classify and risk-assess business functions, processes and assets that are considered critical to the business,
7. Provide security measures that deal with confidentiality, integrity and availability of data and IT systems, as well as physical security and access control,
8. Ensure that the activities are monitored to identify unplanned events that lead to operational or safety-related incidents, as well as managing, monitoring and reporting incidents,
9. Draw up a continuity management plan that includes a description of how operations are to be maintained in different scenarios and how the supplier should communicate in the event of a crisis, test the continuity plans annually and update them if necessary;
10. Develop and regularly test control routines that ensure that security measures are up to date and effective,
11. Develop a threat analysis for payment service activities and regularly train staff on how to use contingency plans, continuity plans and recovery plans and
12. Develop and, if necessary, implement processes and routines to guide and inform PSUs about security risks and error messages related to the payment services provided and PSUs' ability to disable specific payment features.

Chapter 6 Information to Finansinspektionen

Overall assessment of operational risks, security risks and measures

Section 1 A PSP shall annually enter the Financial Supervisory Authority with a report containing a current and comprehensive assessment of the operational risks and security risks associated with the payment services provided by the supplier and a description of the security measures implemented by the supplier to address these risks.

The report shall also include an assessment of the suitability of the security measures implemented by the supplier to address these risks. The report must be received by Swedish Financial Supervisory Authority no later than 21 February

Additional Notes	Sweden requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures. Sweden requires PSPs to provide the Financial Supervision Authority with an up-to-date and comprehensive assessment of the operational and security risks associated with payment services before 21 February.
	Finansinspektionen comments²: FI has informed the European Banking Authority, EBA that FI intends to comply with the EBA Guidelines for Security Measures for Operational Risks and Security Risks for Payment Services. According to the guidelines, a payment service provider must report to the Financial Supervisory Authority if a serious operational incident or security incident has occurred in the business. Parts of the guidelines are announced in the form of binding regulations that enter into force on 1 May 2018, Finansinspektionen's regulations (FFFS 2018: 4) on payment service providers.
	Sweden will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.27.2 Sweden: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Chapter 6 Information to Finansinspektionen

Serious operational incidents or security incidents

Section 4 A PSP shall report to the FSA if a serious operational incident or security incident has occurred in the operation. When reporting, the supplier shall use the form of serious incidents available on the FSA's website.

The information shall be provided in accordance with section A-C of the form, as detailed on the FSA website

1. Within four hours of the occurrence of the incident (Section A),
2. with updated information when there is such and no later than three days from the date of entry into section 1 (section B); and
3. no later than two weeks after the operation usually resumes (section C).

Section 5 A PSP shall inform its PSUs if there is a serious operational incident or security incident that may adversely affect their financial interests. When a PSP informs PSUs, the following requirements shall be met:

1. The information shall be available to the PSU on a durable medium even after the information.
2. The PSP should pay attention to the PSU that there is information about a serious operational incident or security incident that may adversely affect the PSU's financial interests.

Statistical information about fraudulent procedures

Section 2 A PSP shall provide statistical information to the FSA twice a year on fraudulent procedures that have taken place in connection with the use of payment services. The information shall contain

1. Total transaction volume,
2. Total transaction volume related to fraudulent procedures, and
3. An account of data under 1 and 2 divided into
 - a) type of payment service;
 - b) current authentication method,
 - c) type of fraudulent procedure; and
 - d) the transaction was conducted geographically.

The data should refer to the last calendar half and divided by quarter. The supplier shall provide the information by using the forms for reporting available on the FSA website. The information must be received by the Authority no later than 21 February and no later than 21 August.

Registered PSPs and registered electronic money publishers shall provide information according to the first paragraph only once a year, by 21 February at the latest, using the reporting forms available on the FSA's website. The data should relate to the last calendar year and be divided quarterly.

Section 3 Information referred to in Section 2 shall include fraudulent procedures related to completed payment transactions such as

1. Not authorized by the payer,
2. The payer denies that he or she has authorized, or
3. Implemented by the payer being manipulated.

Additional Notes	<p>Sweden requires PSPs to notify the FSA without undue delay of major operational or security incidents. If the incident has affected the user's financial statements, the PSPs will inform them of the mitigating measures to mitigate the incidence.</p> <p>Sweden requires PSPs to provide the FSA, twice a year, with statistical data³ on fraud involving different means of payment. The data should refer to the last calendar half and divided by quarter. The supplier shall provide the information by using the forms for reporting available on the FSA website. The information must be received by the Authority no later than 21 February and no later than 21 August.</p> <p>Finansinspektionen comments⁵: FI will apply after 1 May 2018 to the European Banking Authority, EBA, guidelines for reporting serious incidents under the Second Payment Services Directive. FI has informed EBA that FI intends to comply with the reporting guidelines for serious incidents.</p> <p>According to the guidelines, a payment service provider should report to FI if a serious operational incident or security incident has occurred in the operation. FI proposes that parts of the guidelines be announced in the form of binding regulations that will enter into force on 1 May 2018.</p>
-------------------------	--

4.27.3 Sweden: Regulatory Technical Standards on authentication and communication

SWEDEN

No information

4.28 United Kingdom

On 18 July, 2017, the Prudential Regulation Authority and the Financial Conduct Authority published federal legislation (The Payment Services Regulations 2017, Statutory Instruments No. 752) implementing the PSD2. The legislation enters into force on 13 August, 2017.

COUNTRY	UNITED KINGDOM
Entry into Force	13 August 2018
National Transposition Law	The Payment Services Regulations 2017 http://www.legislation.gov.uk/ukxi/2017/752/pdfs/ukxi_20170752_en.pdf
Competent Authority	Prudential Regulation Authority https://www.bankofengland.co.uk/ Financial Conduct Authority (FCA) https://www.fca.org.uk/
Supervision Authority	Financial Conduct Authority (FCA)
Incident Reporting Authority	
Incident Reporting Channel	Financial Conduct Authority ⁵ : Connect online system https://www.fca.org.uk/firms/connect

4.28.1 United Kingdom: Guidelines on the Security Measures

GUIDELINES ON THE SECURITY MEASURES (ARTICLE 95.3 OF PSD2)

Management of operational and security risks

98.—(1) Each PSP must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides. As part of that framework, the PSP must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) Each PSP must provide to the FCA an updated and comprehensive assessment of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

(3) Such assessment must—

(a) be provided on an annual basis, or at such shorter intervals as the FCA may direct; and

(b) be provided in such form and manner, and contain such information, as the FCA may direct.

Additional Notes

The United Kingdom requires PSPs to have a framework with adequate mitigating measures and control mechanisms to manage operational and security risks related to payment services, including effective incident detection and classification procedures.

The United Kingdom requires PSPs to provide the FCA with an updated and comprehensive assessment of the operational and security risks associated with payment services on an annual or shorter interval basis.

FCA Comments²: On 12 December 2017 the European Banking Authority published final Guidelines (link is external) on security measures for operational and security risks of payments services under the revised Payment Services Directive ('the Guidelines').

All payment service providers (PSPs) will be expected to comply with the Guidelines from 13 January 2018 in addition to the requirements set out in Regulation 98 (Management of operational and security risks) of the Payment Services Regulations 2017. This includes firms undertaking account information and payment initiation services.

The Financial Conduct Authority will comply with these Guidelines. We will consult on our approach to applying these Guidelines and our expectations on PSPs' future reporting requirements in 2018. Businesses wishing to apply for authorisation or registration (and PSPs re-applying) should bear in mind that applications must contain a statement of the applicant's security policy, including a description of the applicant's measures to comply with Regulation 98(1), taking into account the Guidelines.

The United Kingdom will comply with the guideline on the security measures for operational and security risks of payment services issued by the EBA.

4.28.2 United Kingdom: Guidelines on Major Incident Reporting

GUIDELINES ON MAJOR INCIDENT REPORTING (ARTICLE 96.3 OF PSD2)

Incident reporting

99.—(1) If a PSP becomes aware of a major operational or security incident, the PSP must, without undue delay, notify the FCA.

(2) A notification under paragraph (1) must be in such form and manner, and contain such information, as the FCA may direct.

(3) If the incident has or may have an impact on the financial interests of its PSUs, the PSP must, without undue delay, inform its PSUs of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

(4) Upon receipt of the notification referred to in paragraph (1), the FCA must—

(a) without undue delay, provide the relevant details of the incident to the EBA and to the ECB;

(b) notify any other relevant authorities in the UK; and

(c) co-operate with the EBA and the ECB in assessing the relevance of the incident to authorities outside of the UK.

(5) If the FCA receives notification of an incident from the EBA or the ECB it must take any appropriate measures to protect the immediate safety of the financial system.

Reporting requirements

109.—(4) Each authorised payment institution, small payment institution and registered account information service provider, and each credit institution and electronic money institution which is authorised in the United Kingdom and provides payment services, must provide to the FCA statistical data on fraud relating to different means of payment.

(5) Such data must be provided at least once per year, and must be provided in such form as the FCA may direct.

(6) The FCA must provide such data in an aggregated form to the EBA and the ECB.

Additional Notes	The United Kingdom has not made changes with respect to the requirements of the PSD2.
	<p>FCA Comments⁴: The United Kingdom describes in the document of “Payment Services and Electronic Money – Sept 2017” Chapter 13 – Reporting and notifications the procedure for the implementation of the PSRs 2017.</p> <p>Notification of major operational or security incidents under regulation 99</p> <p>15.14.20 D: Payment service providers must comply with the EBA’s Guidelines on incident reporting under the Payment Services Directive as issued on 27 July 2017 where they are addressed to payment service providers.</p>
	FCA adopts the requirements of the EBA guideline and introduces these requirements in the Financial Conduct Authority’s Handbook of rules and guidance.

4.28.3 United Kingdom: Regulatory Technical Standards on authentication and communication

UNITED KINGDOM

Confirmation of availability of funds for card-based payment transactions

68.—(3) The conditions are that—

(c) the PSP making the request complies, for each request, with the authentication and secure communication requirements set out in the RTS adopted under Article 98 of the payment services directive in its communications with the ASPSP.

Access to payment accounts for payment initiation services

69.—(2) Where a payer gives explicit consent in accordance with regulation 67 (consent and withdrawal of consent) for a payment to be executed through a PISP, the payer’s ASPSP must—

(a) communicate securely with the PISP in accordance with the RTS adopted under Article 98 of the payment services directive;

(3) A PISP must—

(d) each time it initiates a payment order, identify itself to the ASPSP and communicate with the ASPSP, the payer and the payee in a secure way in accordance with the RTS adopted under Article 98 of the payment services directive;

Access to payment accounts for account information services

70.—(2) Where a PSU uses an account information service, the PSU’s ASPSP must—

(a) communicate securely with the AISP in accordance with the RTS adopted under Article 98 of the payment services directive;

(3) An AISP must—

(c) for each communication session, identify itself to the ASPSP and communicate securely with the ASPSP and the PSU in accordance with the RTS adopted under Article 98 of the payment services directive;



ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



Catalogue Number TP-07-18-085-EN-N



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-279-0
DOI: 10.2824/98934

