wultra

THE PSD2 COMPLIANCE CHECKLIST

PETR DVOŘÁK, CEO
petr@wultra.com

PLEASE NOTE: This document and the information contained herein is intended as an introduction to PSD2. The document is not for sale and is available free of charge to visitors to the Wultra website. The information contained in the document does not constitute a legal opinion or a commercial offer. The document may only be shared "as is", without changes or additions. Sharing is conditional on crediting Wultra as the source of the information.

INTRODUCTION

Most financial institutions in the European Union have struggled to meet the regulatory requirements of the PSD2 legislation. We understand why this topic causes headaches when dealing with it for the first time. The extensive legal document describing the changes in laws is augmented with a plethora of additional documents published by the European Banking Authority (EBA) or European Commission (EC). These documents provide specific regulatory technical standards and comments and opinions on various aspects of the PSD2 legislation.

PSD2 is a complex, difficult-to-navigate topic. Everything around it is also constantly changing, and as new problems emerge and new interpretations are published, it isn't easy to keep up with the latest developments. Furthermore, PSD2 delivery is typically an unwanted, mandatory project that is often carried out on a tight schedule. As a result, we have seen numerous organizations forget an important topic or miss a critical deadline.

We want to help you stay on top of PSD2. To help you get oriented and more quickly move forward in your projects, we've prepared a checklist of activities that you shouldn't overlook in your PSD2 project.

STRONG CUSTOMER AUTHENTICATION

- ☐ Prepare centralized login page for web applications.
- ☐ Implement new customer authentication methods.
  - ☐ Generate one-time authentication codes.
  - ☐ Authentication codes must use at least two factors (2FA).
  - ☐ Authentication factors must be resilient and independent.
  - ☐ Factors are dynamically linked to amount and payee account.
- ☐ Phase out non-compliant authentication methods.
  - ☐ Deprecate use of HOTP/TOTP (Google Authenticator).
  - ☐ Move away from SMS-based authentication.
- ☐ Adjust authentication system parameters.
  - ☐ Block access after 5 incorrect authentication attempts.
  - ☐ Log user out after 5 minutes of inactivity.
  - ☐ Implement processes for account blocking and unblocking.
- ☐ Ensure that users can gain initial access securely.
  - ☐ Secure onboarding to digital services for new customers.
  - ☐ Secure delivery of new personalized credentials.
  - ☐ Account access recovery procedure for existing customers.
- ☐ Evaluate and implement exemptions from SCA.
  - ☐ Access to account information and transaction history.
  - ☐ Low-value contactless payments at point of sale.
  - ☐ Unattended terminals for transport fares and parking fees.
  - ☐ Trusted beneficiary accounts.
  - ☐ Recurring payments.
  - ☐ Payments to own accounts.
  - ☐ Low-value transactions.
  - ☐ Secure corporate payment protocols.
  - ☐ Low-risk transactions (see transaction risk analysis).
- ☐ Consolidate transaction authorization systems.
- ☐ Use Strong Customer Authentication for e-commerce payments (3DSecure 2.0).

Tip: Use cryptographically strong mobile authenticator to meet PSD2 requirements on customer authentication.

We provide solutions for this area →

HARDEN DEVICE SECURITY

- ☐ Implement device binding and identify known devices.
  - ☐ Keep IP address with each session and operation approval.
  - ☐ Identify previously known devices.
- ☐ Detect compromised multi-purpose devices (mobile, tablet).
  - ☐ Detect root / jailbreak.
  - ☐ Detect application repackaging.
  - ☐ Detect app installation from untrusted source.
  - ☐ Detect attempts of code injection.
  - ☐ Detect and block "debuggers".
  - ☐ Detect emulators and virtualized environments.
  - ☐ Detect outdated OS and missing security patches.
  - ☐ Detect insecure user configurations.
  - ☐ Prevent sensitive data leakage.
  - ☐ Prevent device cloning.
  - ☐ Implement forced app update.
- ☐ Identify signs of malware during authentication sessions.

Tip: PSD2 covers mobile device security requirements briefly. However, it is easy to reach the safe compliance zone by choosing in-app protection to shield your app from various cybersecurity threats.

We can consult on this area and help you pick a vendor →

TRANSACTION RISK ANALYSIS

- ☐ Introduce transaction analysis and anomaly detection.
- ☐ Analyze typical spending patterns and user location.
- ☐ Keep history of transactions and measure fraud rate for various transaction types and compare it to mandatory thresholds.
- ☐ Implement monitoring and reporting to regulatory authorities.

We can consult on this area and help you pick a vendor ➔

IMPLEMENT OPEN BANKING APIS

- ☐ Evaluate and pick open banking standards (i.e., Berlin Group).
- ☐ Select and deploy API gateway.
- ☐ Implement OAuth 2.0 / OpenID Connect federation.
- ☐ Implement PSD2 certificate validation.
- ☐ Implement API for various PSD2 mandates.
  - ☐ AISP - information about payment accounts.
  - ☐ PISP - indirect initiation of payment.
  - ☐ CISP - balance information for card instrument providers.
- ☐ Build public developer portal with API documentation.
- ☐ Implement third-party provider registry.
- ☐ Implement consent management system.
- ☐ Implement developer sandbox.
- ☐ Prepare a backup interface solution, or ask for an exemption.
- ☐ Prepare support channels for third-party providers.

Tip: You can leverage many open and cost-effective building blocks to more quickly build developer portals and open APIs.

We can consult on this area and support your internal decision-making ➔

ORGANIZATIONAL CHANGES

- ☐ Plan for smooth customer migration to new systems.
- ☐ Make transaction fees and charges transparent.
- ☐ Update and publish your general terms of service.
- ☐ Educate users about third-party apps and login flow changes.
- ☐ Train your branch and call center employees.

Tip: Consider the potential of the PSD2 investments and look for ways to turn premium banking APIs into a new revenue stream. Example of such APIs can be customer identification and KYC.

ABOUT THE AUTHOR

Petr Dvořák is the CEO of Wultra. He is an author of two patents in the digital security area and author of the Czech national standard for QR code payments. Outside of work, everything revolves around his passion for motorcycling.

ABOUT WULTRA

Wultra provides leading banks and fintech companies with security solutions for their internet and mobile apps. Thanks to our products, financial institutions can meet compliance with the regulatory requirements and, more importantly, detect and stop malware attacks and protect their apps against a wide range of cyber threats.