A CYBER 1 Company

PSD2 SERVICES

PSD2 SERVICES - WHAT IS IT?

In 2007 EC adopted the original Payment Services Directive ('Directive 2007/64/EC' or 'PSD') to regulate payment services and payment service providers with an aim to increase market competition and stimulate joining of new players in payment industry throughout the EU and EEA enabling faster payments whilst protecting end consumers and increasing their rights with regards to transaction refunds and information transparency.

PSD2 is a revised directive which was adopted in October 2015 and came into force on January 13th 2018 prescribing new rules to promote adoption of new payment technologies, especially for online and mobile payments, better protect end consumers and enable third-party providers to manage finances of bank customers, both consumers and businesses, by using open APIs which banks are mandated to provide as means of access to their customers' accounts. PSD2 also introduced a set of technical standards on strong customer authentication and common and secure communication under Directive 2015/2366 (PSD2) known as Regulatory Technical Standards (RTS). These standards set technical requirements towards measures for the application of strong customer authentication and its exemptions, confidentiality and integrity of the customers personalized security credentials and common open standards of communication (APIs).

PSD2 SERVICES

WHY DO I NEED PSD2 SERVICES?

Both banks and TPPs need to adopt to these standards and take a number of strategic choices, which are not easy but surely expected to increase overall IT costs due to RTS communication and security requirements. This is exactly where DRS can help by providing the technical know how and experience in payments industry in conjunction with its advisory and assurance cybersecurity services to ensure that all payment parties are protected. In practice this implies the implementation of a series of technical and organizational measures aimed at reducing the security risks of various internal and external threats and compromising consumer personal data managed by payment service providers apps and exchanged with other payment entities. One of the biggest challenges for companies is to identify technical weaknesses and disadvantages in their applications and systems and to identify concrete technical measures which are necessary to protect the system against unauthorized and malicious activities and maintain confidentiality and integrity of data.

Being it a mobile or web application or a payment framework within your payment environment or a complex system, taking into consideration the eco-system context, DRS can carry out a comprehensive analysis of the implemented system and related processes, its security controls and their effectiveness by performing rigorous testing, ranging from penetration testing, application security assessments, code reviews, vulnerability assessments and thorough information system audits necessary for compliance. Not being a final list of topics on the overall security list, in light of PSD2 we shall especially pay attention in assessing and providing guidance on certain parts of your systems and processes;

Interfaces, APIs and data | Authentication processes and SCA | Authentication codes management and dynamic linking
Authorisation processes | Fraud monitoring | Payment account and transaction data availability | Certificates
Card transactions | Secure execution environment

Our team of highly experienced technical personnel with vast experience in the banking and payments industry, as well as the required accreditations and knowledge will provide you with a detailed analysis report and guidance that will enable the system's security enhancement and, consequentially, will pinpoint exact PSD2 requirements that need to be addressed to achieve compliance.

A CYBER 1 Company

PSD2 SERVICES

When do i need it?

PSD2 came into force on January 13th 2018 which means involved parties are mandated to enable the "access to accounts" services, except for the security measures outlined in the RTS which are now in a "transitional" period. Payment service providers and other market players need this transition period to upgrade their payments security systems so that they meet the RTS requirements, which will become applicable 18 months after the date of entry into force of the RTS, i.e. once the RTS, subject to the agreement of the Council and the European Parliament, is published in the Official Journal of the EU, scheduled for September, 2019.

This means that the PSD2 provisions on strong customer authentication (SCA) and on secure communication, which are directly specified in the RTS, will not apply immediately, i.e. the application of security measures in Articles 65, 67 and 97 of PSD2 is postponed until the RTS becomes applicable. However, those parts of Articles 65, 67 and 97 that are not dependent on the RTS will apply as of 13 January 2018. The final version of RTS was published on November 27th, 2017 thus leaving enough time to payment service providers to take action to develop a compliance strategy and implement effective security solutions for electronic remote payment transactions.