Turn PSD2 and GDPR into business opportunities

How to manage consent under PSD2

Both business- and compliance-wise, the year 2018 will lead to major changes in the financial industry. With PSD2 and GDPR, two major EU regulations are coming into force at more or less the same time.

While two separate initiatives, the Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR) have important overlaps as both lay down **strong requirements on data protection and consumer's consent for data handling** by organisations.
First and foremost, PSD2 is to open up the financial (or: banking) industry to third parties in an attempt to boost competition and – as a consequence – innovation. With **explicit consumer's consent**, these third parties (in PSD2 referred to as Third Party Providers or TPPs) are allowed free access to specific services that used to be the exclusive right of banks.

Payment Initiation Service (PIS)
On top of access to bank account details, TPPs are allowed to provide consumers the option to initiate payments. Again, via the TPP's website or user app and without visiting the bank's channels. It allows for a payment service which is free of charge and can be used to build innovative products.

Account Information Service (AIS)
With this service, TPPs can offer consumers direct access to their bank accounts via the TPP's website or user app. Without having to visit the bank's channels first. The advantage for consumers here is that it allows for one single point of access to a wide variety of banks. Moreover, TPPs can build innovative services on top of this AIS.

The importance of data protection and explicit consumer consent in PSD2

Especially for conservative and highly secured species as banks, allowing 'strangers' (free) entrance to personal data from their core infrastructure does not feel comfortable. Most surprisingly, no specific requirements are called upon in the directive. This is where the GDPR comes into play.

GDPR creates a regulatory framework to protect personal data. This EU regulation states that consent needs to be "freely given, specific, informed and unambiguously". And GDPR requires organisations to offer consumers the possibility to view, edit, download and delete all personal data (including their consent settings) that are being held on them.

Based on the requirements set by PSD2 and GDPR, TPPs can either obtain a consumer's consent or use direct consent APIs bypassing the contractual consent part. This would result in banks being unaware of whether and – if so – what type of consent has been granted by the consumer. And as data controller under GDPR, banks are held fully responsible for this data. Having no agreement in place would result in not being compliant. As such, this will unlikely happen.

The central theme for all three challenges is **consumer data management.** To succeed, Consumer Identity & Access Management (CIAM) must become the foundation for commercial success and compliance of any insurer. Turn this page to find out how iWelcome helps insurers overcome these challenges.

Say goodbye to consent issues with iWelcome's consent lifecycle management solution

In practice, TPPs will most likely be the ones initiating consumer's consent while banks will remain responsible for confirming the consent directly with their customers. To prevent messing up the customer journey, the latter will happen via so-called consent APIs, granted by banks to TPPs, who will incorporate it into their websites or user apps.

All consent details as the identity of the TPP, the types of data consumers request to share and the consent retention period after which new consent has to be obtained. As banks are per definition complex organisations with data stored in different systems, it will prove hard to perform proper consent lifecycle management by the bank without help. Luckily, banks can turn to iWelcome for support. With iWelcome's consent lifecycle management service, banks don't have to worry about storing different data in separate IT systems. A high-level overview of this situation is shown in figure 1 below.

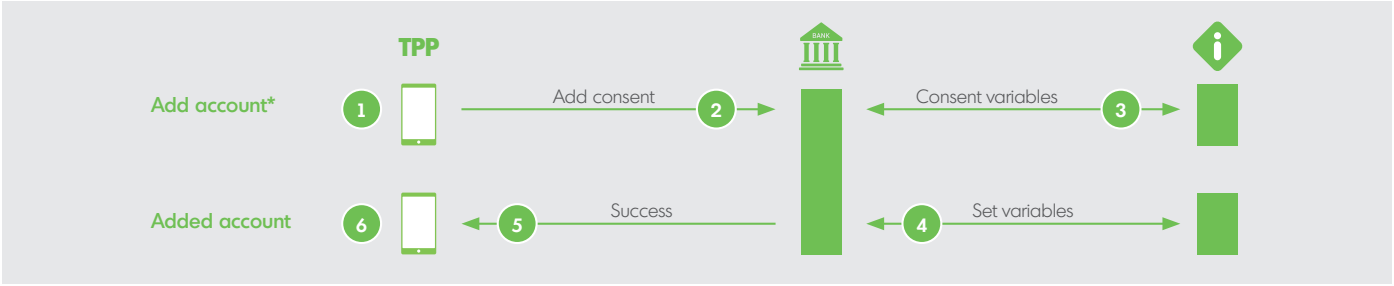


Figure 1: The process of consent provision

When consent has been granted, consumers can exercise the account information or payment initiation service of the TPP. The TPP will then process the information request to the respective bank to see whether consent has been obtained. The bank then verifies whether consent has been granted and belongs to this person, using iWelcome's consent API (see figure 2).

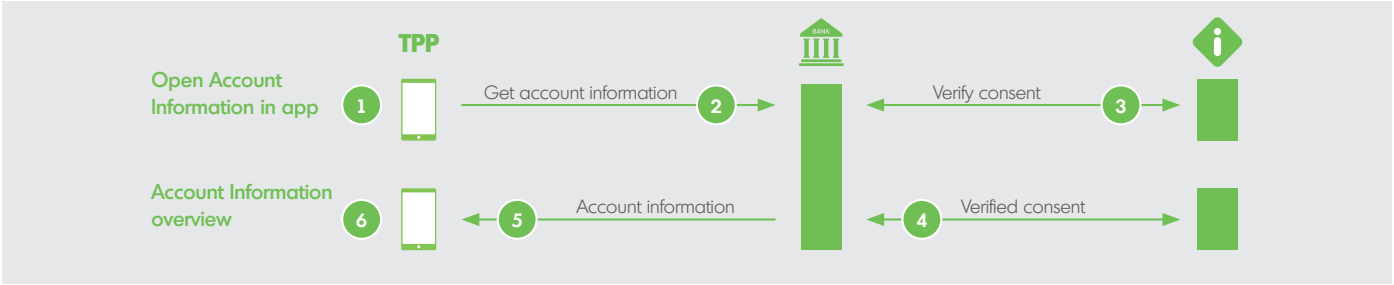
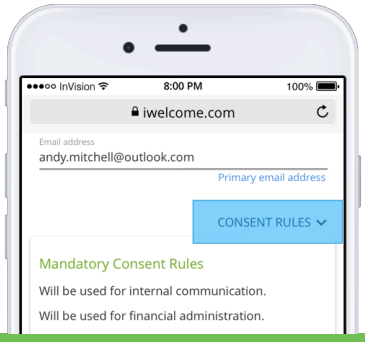


Figure 2: Account Information Service with consent verification

On top of that, using iWelcome's solution allows banks to easily offer their consumers the option to view, edit, download and/or delete all personal identity data (including consent information) the bank holds on them. This iWelcome service can be delivered both white-label or via RESTful APIs.



About iWelcome

iWelcome provides Identity as-a-Service for frictionless privacy-protected consumer services and security-enabled workforce processes. iWelcome is the only European born Identity Platform - headquartered in Europe, backed by European investors and specifically serving enterprise customers doing business in Europe. Millions of consumers and hundreds of thousands of employees - across industries like banking, insurance, utilities, media & publishing, travel & services, retail/ e-tail and Governments & Non-Profit – rely on iWelcome on a daily basis. Analysts like Gartner and KuppingerCole have recognised iWelcome as a worldwide Product and Innovation Leader with "Excellence" ratings.

Building truly winning partnerships with its customers, iWelcome offers lowest Total Cost of Ownership and a time-to-service in weeks. Applying Best-of-Breed Private Cloud Technology, customers benefit from both ends: using a SaaS service while not having to share critical resources.