COMPLIANCE & RISK
CONGRES | 2017

Open Banking and APIs
How to stay in control?

Arno Voerman

20 June 2017

VanDoorne
Advocaten • Notarissen • Fiscalisten

PSD2 as driver for APIs/open banking

Targeting developers

PSD2 is the tipping point for API technology to break through into the financial sector. At first glance, they may seem innovative, but open APIs have been an established feature outside the financial sector for quite some time. In fact, a real API economy exists which banks are only now entering gradually. Besides the mandatory PSD2 APIs, banks such as BBVA, Capital One and Crédit Agricole are unveiling other products and services via APIs. APIs have long been more than mere IT interfaces, and now represent a new product and channel catering for new and existing clients such as developers.

From closed to open banking

PSD2 marks the beginning of a wider transformation in the financial sector, and signals a shift towards a more open financial sector with more APIs than just those required by PSD2 – it's a new trend popularly known as open banking.

(PSD2 is not just about PSD2 any more, Blog Laurens Hamerlinck - 30 June 2016)

APIs

RIJKS MUSEUM

Toegang tot de API

Om toegang te krijgen tot de data en afbeeldingen dien je een API key aan te vragen. Dan kan je doen bij bij je geavanceerde instellingen in je Rijksstudio account (https://www.rijksmuseum.nl/rijksstudio). Je krijg dan direct een code. Deze code heb je nodig om gebruik te maken van de api's.

Example request

The following request will fetch all of the public data of The Nightwatch, in Dutch using the format JSON:

```
https://www.rijksmuseum.nl/api/nl/collection/sk-c-5?key=fakekey&format=json
```

LinkedIn

Step 2 - Retrieve basic profile data

Once you have obtained a valid access token for the user, you can use the following REST API call to retrieve basic profile data for the user:

GET https://api.linkedin.com/v1/people/~?format=json

Wikipedia: In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. **In general terms, it's a set of clearly defined methods of communication between various software components**. A good API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer. An API may be for a web-based system, operating system, database system, computer hardware, or software library. An API specification can take many forms, but often includes specifications for routines, data structures, object classes, variables, or remote calls. POSIX, Microsoft Windows API, the C++ Standard Template Library, and Java APIs are examples of different forms of APIs. **Documentation for the API is usually provided to facilitate usage.** The status of APIs in intellectual property law is controversial.

APIs and Banking as a platform

solarisBank

"Our services are like Lego bricks: our partners can pick the bricks they require and assemble custom solutions to fit their business needs. Partners can access Solaris Platform services via our easy-to-implement API. The frictionless and straight-forward integration enables solarisBank partners to launch quickly and concentrate on their core business. Of course, we want to reassure our partners that we are fully committed to data privacy and complying with regulations. In fact, enabling compliance for our partners is one of our key offerings."

— Andreas Bittner (Managing Director solarisBank)

Integrating to your Fire account

In addition to accessing your **Fire** account via our online application, you may also connect your systems directly to your **Fire** account using our API.

Our API enables your in-house application to retrieve and display data from your **Fire** account. You create permission based tokens so different applications can access different data in **Fire**. You may also configure real time messages to be sent from your **Fire** account to your own applications when certain events occur – e.g. a lodgement is received.

We make it easy for businesses to access the transactions and data in their accounts.

Ralph Hamers, ceo en bestuursvoorzitter van de ING Groep kijkt uit naar de invoering van de Europese regelgeving rond PSD2, waarschijnlijk januari 2018. De bank experimenteert al met de mogelijkheden op Europese markten die inmiddels een open bankensysteem kennen zoals Spanje, waar ING het leenplatform Kabbage ondersteunt. (FD, 15 april 2016)

Open Banking and APIs

Areas of law

- **Contract** law
- **IP**-law
- **Data protection** (2018: GDPR)
- **Open data regulations**
- (Financial) **Regulatory** (2018: PSD2)
- **Competition** law

Challenges

- PSD2 and **Mandatory Access** (XS2A)
- **How** to provide access?
- **Data protection regulations**
- **Liability**
- **How to verify** Third Party Providers (TPPs)?

3:17 Wft:
- *Beheerste en integere bedrijfsuitoefening*
- *Beheersen van bedrijfsprocessen en bedrijfsrisico's*

20 (2) Bpr Wft:
Waarborgen van integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking

13 Wbp:
Passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking

25 AVG:
- *Passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.*
- *Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel ("by default") niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.*

32 AVG:
De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

How to start with APIs?

Four key questions

- What to share?
- Can I share?
- With who to share?
- How to share?

Impact PSD2 and GDPR

How to start with APIs?
Key legal questions and challenges

What to share?	Can I share?	With who?	How to share?
Open data	**Consent**: • specific, • Informed • and freely given	**Open access**	**Contract**
Customer transaction data	**Compliance** with a legal obligation	Only **authorized** persons	**API Terms & Conditions (opt-in)**
Customer reference data	**Legitimate interests**		**Schemes/Rulebook**
Aggregated data **Sensitive commercial** data **Challenge**: • **Personal** data • **Sensitive** data	**Challenges:** • What if 3PP has **no contract** with customer? • **Silent** parties? • **Explicit consent for sensitive data** • Consent can be **withdrawn** • **PSD2**: **explicit consent**	**Challenge scope consent**: • **Who** are you providing authorisation to? • **What** are you providing authorisation for? • **How** long will the authorisation last for?	**Challenge PSD2**: • Bank **must allow access** to the account • Bank may **not require a contract**

API-strategy: legal challenges

Liability (who to blame?)
- Data breach & cyber security threats
- Correctness: “as is” basis

Data protection compliance:
- GDPR
- information duties
- data transfer outside EEA
- data processing in the course of providing advanced PIS/AIS services)

Database protection (against structural and substantial data requests) vs. XS2A

Bank/data provider trademark use by 3PP

API-strategy: legal check list and advice

- Determine scope of access
- Verify which data can be shared
- Verify IP-rights
- Change customer agreements for future use
- Determine the level of openness
- Determine the required security measures
- Check robustness of IT-architecture
- Check on compliance data protection rules and financial regulatory

Advice:

- Provide for **controlled** access
  - Contract;
  - T&Cs
  - Schemes/Rule Books
- But check PSD2 Impact

Contact

Arno Voerman
Partner, Payments & FinTech
t +31 20 6789 250
m +31 61 1388 538
Voerman@vandoorne.com

AMSTERDAM
Van Doorne N.V.
Jachthavenweg 121
1081 KM Amsterdam

P.O. Box 75265
1070 AG Amsterdam
The Netherlands

t +31 (0)20 6789 123
info@vandoorne.com
www.vandoorne.com

LONDON
Van Doorne UK B.V.
125 Old Broad Street
London EC2N 1AR
United Kingdom

t +44 20 7073 0465
london@vandoorne.com
www.vandoorne.com

ASSOCIATION WITH
VANEPS KUNNEMAN VANDOORNE

ARUBA I BONAIRE I CURACAO I ST. MAARTEN
DUTCH CARIBBEAN DESK (AMSTERDAM)

info@ekvandoorne.com
www.ekvandoorne.com

VanDoorne
Advocaten • Notarissen • Fiscalisten