TaylorWessing

FIDA Regulation: a glimpse into Open Finance

Dr. Verena Ritter-Döring, Miroslav Đurić LL.M.

15.11.2023

Agenda

1 Open Finance in a nutshell

2 Overview of the proposed framework

3 Financial Information Service Providers

4 Access to data under FIDAR

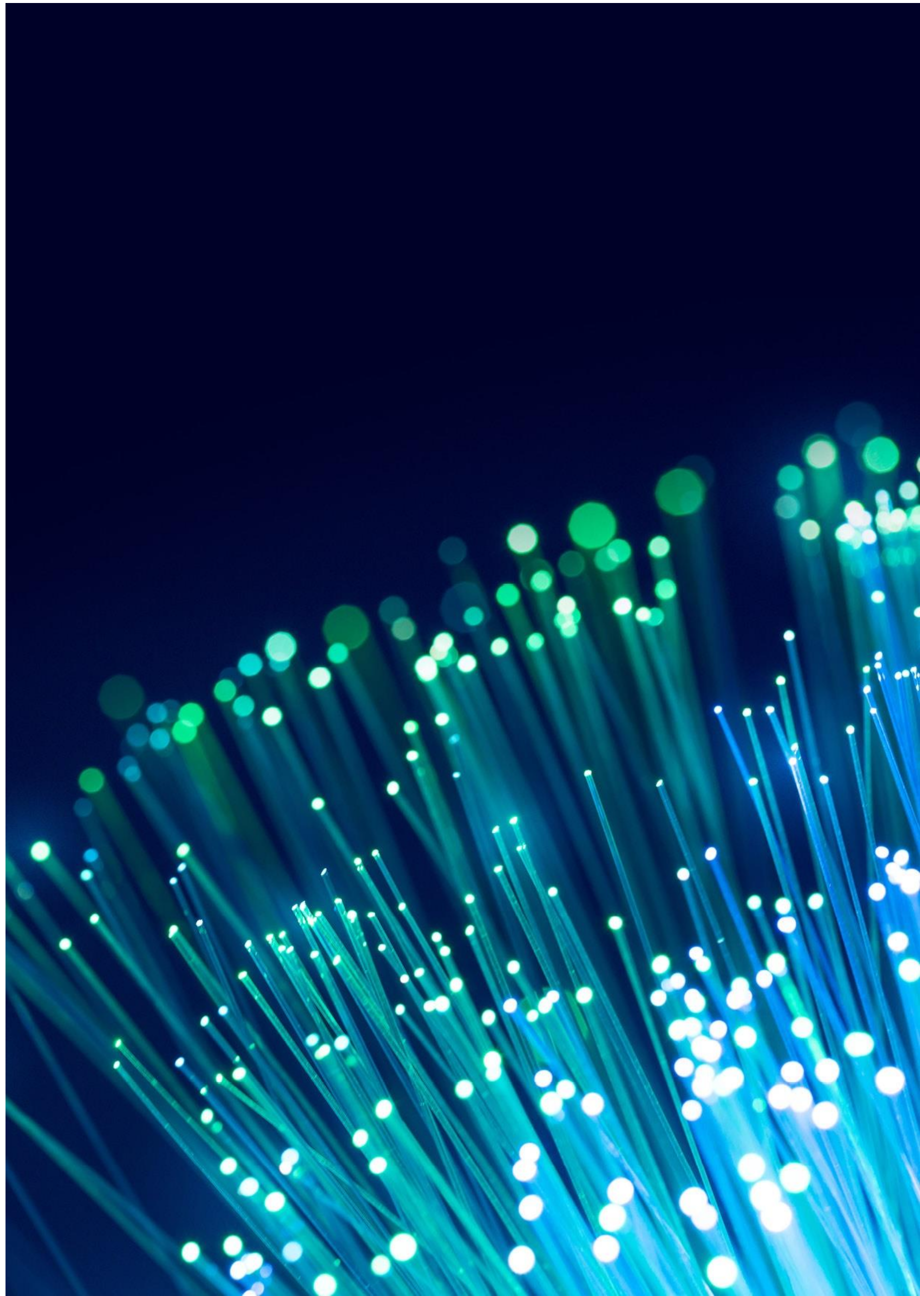
5 Practical impact on the industry

Open Finance in a nutshell

Open Banking

- Introduced as a part of the PSD2 framework, enables new entrants to get access to the EU payments market
- PISPs – able to initiate payment transactions through customers' existing payment accounts
- AISPs – able to extract data from various payment accounts of the customer and provide an aggregate overview of all accounts in one place

- **Instant checkout:** customers allow a merchant through a PISP to initiate the payment instantly (and bypass any need to e.g. re-enter card details for every transaction).
- **Variable Recurring Payments:** money in various accounts of a customer is automatically shifted around to ensure your funds are optimized (e.g. upon identification of a pending payment and lack of funds, the system automatically shifts money from a savings account to the payment account to cover the payment and prevent overdraft)



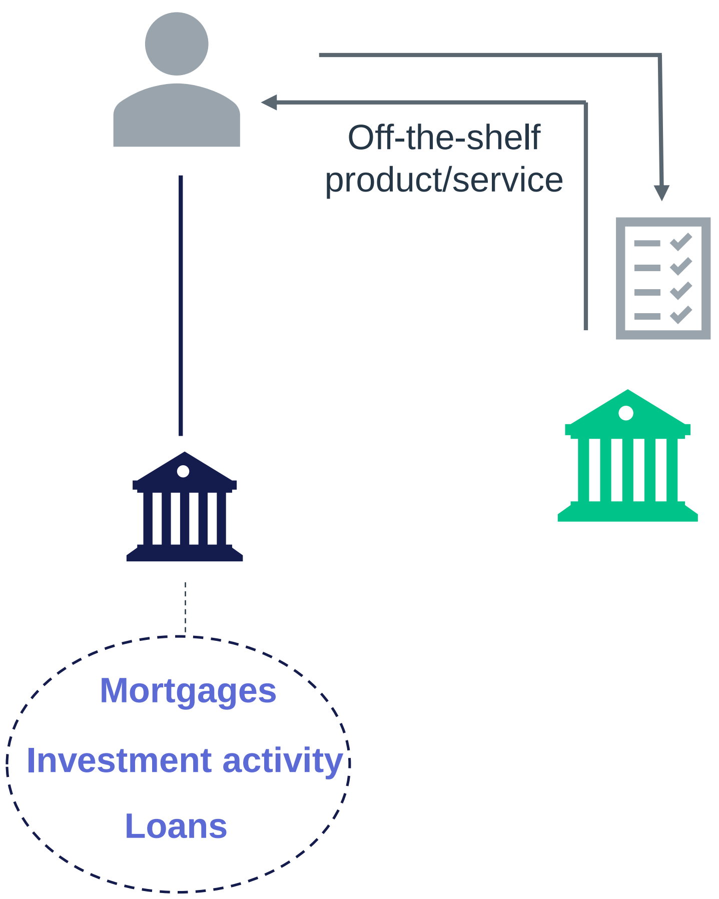
The next step of the journey – Open Finance

- Open Finance is a term used to describe the **extension of open banking data-sharing principles** to enable consent based sharing and use of customers' data across a broader range of financial products (beyond payment accounts)
- Open Finance relies on business-to-business data sharing via APIs which increases competition between financial service providers and provides customers with a greater level of flexibility and choice when using financial services
- Scope: financial instruments, mortgages, insurance products etc.
- FIDA Regulation - sectoral building block that fits into broader European strategy for data driven economy
- Aligned with GDPR, Data Governance Act and Data Act

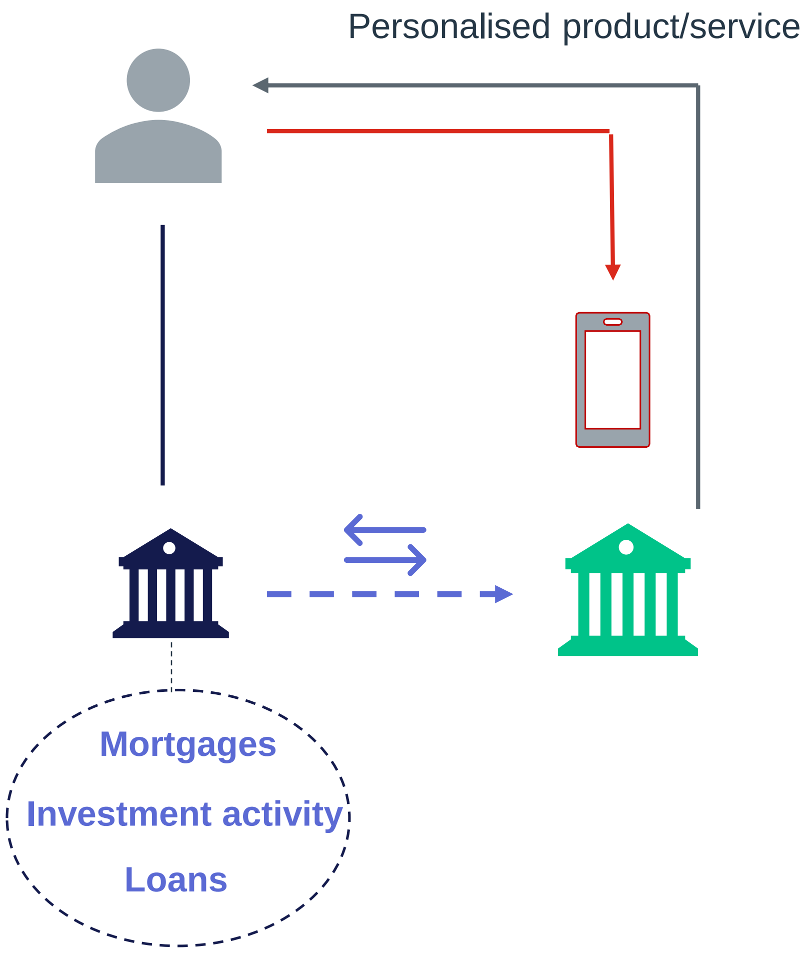
- Giving customers control over their data and enabling them to use it for their benefits
- Enabling customers to get access to personalised service/product offering from day 1
- Improving competitiveness in the financial services sector
- Regulating access to data by unregualted platform providers

The next step of the journey – Open Finance

Current situation



Open Finance



- ✓ Automated onbaording procedure (from KYC to creation of a customer profile)
- ✓ Finding most suitable product/service for the client based on the previous data
- ✓ Personalised service/product offering from day 1

Overview of the proposed framework

Financial Data Access Regulation

- On 28 June 2023, the Commission published its payments and financial data access package as part of which the proposal for a Financial Data Access Regulation was published (FIDA Regulation)
- FIDAR shall create a framework for controlled and **consent-based sharing of financial data**

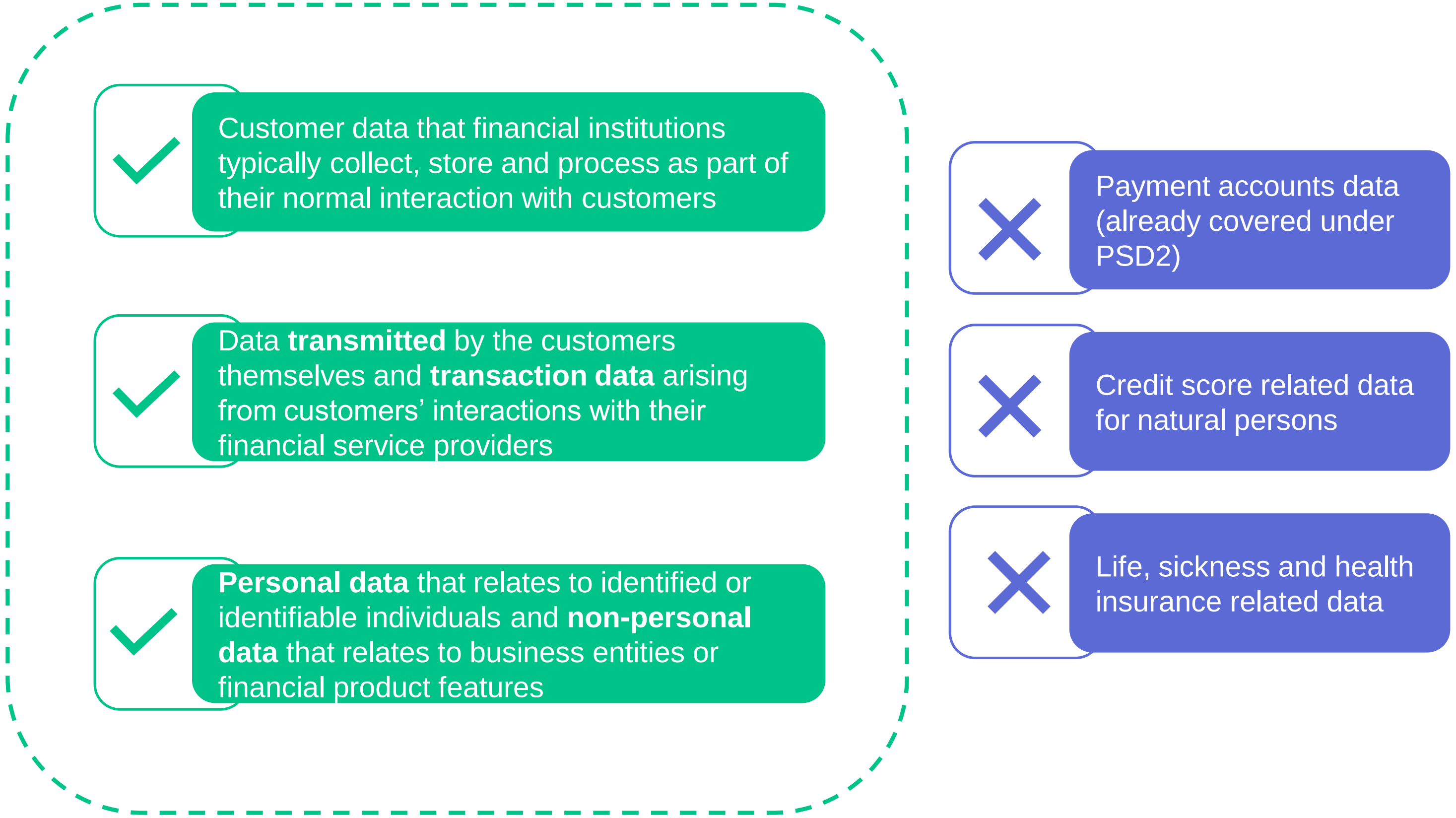
- Wide scope of application: catches every corner of the financial services sector (investment services, banking, insurance, asset management)
- Payment accounts data not covered (already regulated under PSD2)
- Open Banking & Open Finance frameworks will coexist alongside one another

- First draft, that yet needs to find its way through the EU legislative making process
- **Starts to apply 24 months after entry into force**

Scope of application

In-scope data

- Mortgage credit agreements, loans, and accounts (except payment account related data that is already regulated under PSD2).
- Savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate and other related financial assets as well as economic benefits derived from such assets including data processed as part of suitability and appropriateness assessments under MiFID II;
- Pension rights in occupational pension schemes within the scope of Institutions for Occupational Retirement Provision II and Solvency II;
- Non-life insurance products (e.g. car insurance);
- Creditworthiness assessments of companies (where data is collected as part of a loan application process or based on a request for a credit rating).



✓ Customer data that financial institutions typically collect, store and process as part of their normal interaction with customers

✓ Data **transmitted** by the customers themselves and **transaction data** arising from customers' interactions with their financial service providers

✓ **Personal data** that relates to identified or identifiable individuals and **non-personal data** that relates to business entities or financial product features

✗ Payment accounts data (already covered under PSD2)

✗ Credit score related data for natural persons

✗ Life, sickness and health insurance related data

Data holders and data users

Financial Institutions

- Credit institutions
- E-money institutions
- Payment institutions
- MiFID II investment firms
- Crypto-asset service providers (MiCAR)
- Issuers of asset-referenced tokens (MiCAR)
- UCITS ManCos and AIFMs
- Insurance companies and insurance intermediaries
- IORPs
- Crowdfunding service providers
- Credit rating agencies
- PEPP providers

Data holders

- Financial institution other than an account information service provider that collects, stores and otherwise processes in-scope customer data

Data users

- Any of the entities listed on the left-hand side of the slide, that, following the permission of a customer, has lawful access to customer data

Who can access customers' data under the proposed framework?

Customer

- Can request access to their data held by a financial institution that is deemed as "data holder"

Data User

- Licensed financial institutions
- Licensed Financial Information Service Providers (*new category of third party service providers)

Special Access

- Access to data for purposes agreed with a customer for specific product or service
- Limitation: personal data limited to what is necessary only

Financial Information Service Providers

Financial Information Service Providers (FISPs)

What are FISPs?

- Data user that is authorized under the proposed framework to access the customer data for the provision of financial information services;
- **Example:** online platforms that enable customers to have aggregated overview of their accounts and positions across various institutions in one dashboard
- AISPs under PSD2 framework (payment accounts) FISPs (investment, insurance, mortgage products)

Licensing framework

- With the aim of ensuring the highest level of protection of customers' financial data, EU Commission proposes to bring entities providing currently unregulated financial information services within the regulatory perimeter
- FISPs will be the only type of entities alongside regulated financial institutions that will have access to customers' data under the proposed framework
- FISPs will need to obtain authorisation from their local NCAs prior to commencing with the provision of financial information services in the EU;

Authorisation requirements for FISPs

Substance requirements

- Need to be incorporated in the EU or
- Designate, in writing, a legal or natural person as their legal representative in one of the Member States from where the financial information service provider intends to access financial data (liable for non-compliance)

Insurance / Capital Requirements

- FISPs need to hold a professional indemnity insurance covering the territories in which they access data, or some other comparable guarantee, covering their liability resulting from fraudulent/non-authorized access to data
- Alternatively, FISPs can hold initial capital of EUR 50 000
- Initial capital can be replaced by a professional indemnity insurance or other comparable guarantee after it commences its activity as financial information service provider

Operational requirements

- Need to establish proper governance and internal control mechanisms (incl. administrative, risk management, accounting, fraud prevention procedures)
- Compliance with business continuity, digital operational resilience, outsourcing and incident reporting requirements (subject to DORA)
- ESAs mandated to develop RTS specifying authorisation requirements and necessary documentation in more detail

Cross border operation

- Third country applicants may get authorisation provided that they have designated a representative in the EU and that they have demonstrated compliance with key authorisation requirements
- FISPs can access data of customers from other EU Member States, following a simple notification procedure (EU Passport)
- EBA will create and maintain a register of all authorised FISPs including information on those that are operating based on the EU Passport

Access to data under FIDAR

Obligations on data holders (financial institutions)

Access right

- Upon request, financial institutions will be obliged to make customers' data available to data users that are requesting access to data based on customers' consent
- The customer data shall be made available to the data user without undue delay, continuously and in real-time
- Data holders will be allowed to claim compensation from a data user for making customer data available only if the customer data is made available to a data user in accordance with the rules and modalities of a financial data sharing scheme (more on this later)

Provision of data

When making customers' data available, financial institutions must:

- request data users to demonstrate that they have obtained the permission of the customer to access the customer data held by the data holder
- make customer data available to the data user in a format based on generally recognised standards and at least in the same quality available to themselves
- communicate securely with the data user by ensuring an appropriate level of security for the processing and transmission of customer data
- provide the customer with a permission dashboard to monitor and manage permissions
- respect the confidentiality of trade secrets and intellectual property rights when customer data is accessed

Obligations on data users

Access to customers' data

- Financial institutions and FISPs only
- Allowed to access customer data only for the purpose and under the conditions they have been granted permission
- Customers can withdraw their permission at any point
- The processing of personal data (within the meaning of GDPR) shall be limited to what is necessary
- Prohibited from processing customer data for advertising purposes, except for direct marketing in accordance with Union and national law;
- Where the data user is part of a group of companies, customer data shall only be accessed and processed by the entity of the group that acts as a data user.

Safeguards

- Put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal customer data that is unlawful under Union law or the national law of a Member State
- Take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal customer data;
- Delete customer data when it is no longer necessary for the purposes for which the permission has been granted by a customer
- Prevent the transfer of non personal data to third parties where no legal basis exist (personal data covered under GDPR)

Permission dashboards

Data holders will be required to provide customers with a permission dashboard to monitor and manage the permissions a customer has provided to data users. The permission dashboard shall:

- provide the customer with an overview of each ongoing permission given to data users :
- allow the customer to withdraw a permission given to a data user;
- allow the customer to re-establish any permission withdrawn;
- include a record of permissions that have been withdrawn or have expired for a duration of two years.

- The data holder shall ensure that the permission dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the customer.
- The data holder and the data user for which permission has been granted by a customer shall cooperate to make information available to the customer via the dashboard in real-time
- The data holder shall inform the data user of changes made to a permission concerning that data user made by a customer via the dashboard
- A data user shall inform the data holder of a new permission granted by a customer regarding customer data held by that data holder,

Financial Data Sharing Schemes

- Within 18 months from the entry into force, data holders and data users shall become members of a financial data sharing scheme governing access to the customer data (may become members of more than one)
- Industry “self governing body” whose main aim would be to bring together data holders, data users and consumer organizations to foster development of common data sharing and industry recognized interface standards as well as a joint standardized contractual framework governing access to specific datasets.
- It should consist of a collective contractual agreement between data holders and data users with the objective of promoting efficiency and technical innovation in financial data sharing to the benefit of customers.

- Financial data sharing schemes, shall (among other):
- establish a model to determine the maximum compensation that a data holder is entitled to charge for making data available through an appropriate technical interface for data sharing with data users in line with the common standards
- Determine the contractual liability of its members, including in case the data is inaccurate, or of inadequate quality, or data security is compromised or the data are misused. In case of personal data, the liability provisions of the financial data sharing scheme shall be in accordance with GDPR
- Provide for an independent, impartial, transparent and effective dispute resolution system to resolve disputes among scheme members and membership issues

Practical considerations

Interplay with other key pieces of EU legislation

Digital Operational Resilience Act (DORA)

- Both financial institutions and FISPs will be subject to new requirements on digital operational resilience under the new Digital Operational Resilience Act (DORA)
- Any data sharing infrastructure must be in compliance with the requirements for the internal compliance framework on digital operational resilience (ICT risk management, business continuity, incident reporting etc.)

Data Act & GDPR

- Processing of personal data remains regulated by the GDPR (financial institutions and FISPs need to maintain compliance)
- FIDAR is part of a broader policy initiative of the EU Commission
- FIDAR complements the proposed EU Data Act when it comes to B2B sharing of non-personal data

Outsourcing requirements

- DORA outsourcing requirements will apply (incl. RTS on outsourcing)
- Existing outsourcing requirements (based on EBA Guidelines and national regulations) will continue to apply (and will likely be amended) for all DORA-unrelated agreements

PSD3/PSR

- The proposed Payment Services Regulation (PSR), that will replace PSD2 in this area, will regulate data sharing related to payment accounts data
- FIDAR will not replace the existing regulatory framework on open banking
- Both open finance and open banking framework will coexist alongside one another

Impact on the industry

1

Legal impact

- Will impact the industry in much more significant way than the open banking framework under PSD2 (due to a wide scope of application)
- Look at your contractual arrangements, internal procedures, alignment with other sector specific regulations (main areas of work)
- What are the implementation challenges? – navigating several regulatory change projects at the same time
- FISPs – prepare to enter into a regulated space (licensing, ongoing compliance)

2

Operational & Technical Impact

- Huge implementation work is expected
- IT infrastructure, interfaces and internal processes for data sharing need to be developed
- Arrangements with third party service providers (DORA impact)

3

Impact on business models

- Institutions will need to become able to leverage the use of customers' data
- Develop product and service offering that can be tailored to new customers' needs from day one (based on obtained data)
- We may well expect a rising number of new market entrants who are focused on operating in the data driven economy

Thank you!

Dr. Verena Ritter-Döring

Partner, Head of Financial Services Regulatory

Rechtsanwältin (Germany)

Frankfurt am Main, Germany

+ 49 69 997130-404
v.ritter-doering@taylorwessing.com

Miroslav Đurić LL.M.

Associate, Financial Services Regulatory

Solicitor (England & Wales)
Solicitor (Ireland), REL (Germany)

Frankfurt am Main, Germany

+ 49 69 997130
m.duric@taylorwessing.com

Europe > Middle East > Asia

taylorwessing.com

This publication is not intended to constitute legal advice. Taylor Wessing entitites operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at taylorwessing.com/en/legal/regulatory-information.