SETTERWALLS

FinTech Report 2023

SETTERWALLS

Compliance, Compliance and Compliance!

In the ever-evolving FinTech landscape, 2023 is the year of regulatory reflections and as such this is the principal area of focus for this report. Navigating complex (both existing and new) legal and regulatory terrain (often cross-border) which accompanies rapid tech transformation, is indeed a huge contemporary challenge. Thus, we believe it to be topical to elaborate upon upcoming new legislative requirements and trends. Our regulatory focused report also includes a complementary interview with Qliro and its day-to-day 'best practice' compliance guidance.

Despite the heavily regulatory focus, it would be remiss of us to not also afford adequate attention to the new "Sheriff in town", namely Artificial Intelligence (AI). We therefore also dedicate space in this report to allow us to reflect on AI's exponential rise and the legal implications of its seemingly limitless applicability.

Please do join us on a high-level journey through the legal dimensions of FinTech in 2023. We seek to explore the intricate interplay between innovation and regulation, and the pivotal role that legal frameworks play in shaping the future of FinTech and its ancillary evolutions, such as AI. Thus, we hope to empower FinTech industry stakeholders with the knowledge and tools needed to thrive and drive positive change throughout the ecosystem.

So, without any further delay, it is our pleasure to present to you Setterwalls' FinTech Report 2023. We very much hope that you will enjoy it!

- **Important take-aways of the EU Commission's proposal for a new Payments Package**
- **Tokenization of Financial Instruments: The Future of Finance**
- **Consumer terms in the crypto market – the Swedish Consumer Agency's review and conclusions of cryptocurrency asset intermediaries' terms and conditions**
- **Building a strong foundation: how legal best supports first line operations for business success - interview with Qliro**
- **Unraveling DORA: Cyber Resilience Requirements in Digital Finance**
- **Open Finance under FIDA – What to Expect from a Swedish Perspectiv**
- **Generative AI is here – what to consider for companies when using generative AI technology.**

Yours sincerely,
Joacim Johannesson
Partner, and Head of Setterwalls' FinTech team

Important take-aways of the EU Commission's proposal for a new Payments Package

*The EU Commission has put forward proposals to amend and modernise the current Second **Payment Services Directive** (PSD2), thus becoming **PSD3,** and to establish a thereto related **Payment Services Regulation**. The purposes of the Commission's proposals are, inter alia, to improve the competition within the payment industry and to ensure that consumers may continue to make electronic payments in a secure manner, within the EU, domestically and cross-border. In this article, we look closer at some of the most interesting features of the proposed rules.*

Background – evaluating the impact and application of PSD2

PSD2 is the current EU legal framework regulating retail payments in the Union. In general, the PSD2 intends to regulate the fluctuating types of payment services and to improve the level of consumer protection and security, aiming to, inter alia:

- ensure a competitive and level playing field between current and new providers of card-, internet- and mobile payments;
- increase the efficiency, transparency, and choice of payment instruments for payment service users (mainly consumers); and
- facilitate the provision of different internet, card, and mobile payment services.

A targeted consultation of the application and impact of the PSD2 took place during 2022.[1] The purpose was to inform the EU Commission on the application and impact of the

1 finance-2022-psd2-review (europa.eu)

PSD2, and to assess whether the PSD2 remains fit for purpose, taking into consideration certain developments in the payment market, payment users' needs, including charges, scope, and access to payment systems. The evaluation concluded, inter alia, that there is an unlevel playing field between Payment Service Providers (PSPs), partly due to the lack of direct access by non-bank PSPs to certain key systems necessary to finalise payments.[2]

Following this preparatory work, the Commission has proposed certain amendments to the PSD2 for the purpose of adapting applicable legislations to evolving payments services, the evolving payment landscape and technological advancements. The Commission's proposal also aims to improve consumer protection and the security and accessibility of different payment services.

The proposed PSD3 & PSR

General

On June 28, 2023, the Commission proposed an amended payment services package, including a proposal for a third payments services directive (PSD3) and a new payment services Regulation (PSR), intended to replace the PSD2 and the Electronic Money Directive. The proposed approach would thus have the effect that payment services and electronic money would become subject to one single legislative regime.

The proposed PSR contains the general rules in relation to e.g., operational and information requirements for PSPs and sanctions for PSPs, while the proposed PSD3 mainly regulates the authorisation process for Payment Institutions (PIs) and the supervisory system.

The PSR will encompass rules pertaining to all activities for PSPs, integrating certain provisions from the currently applicable Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) and Common and Secure open standards of Communication (CSC), as well as guidelines and opinions from the EBA. Furthermore, PSR will (as an EU regulation) become a single directly applicable legal framework covering all operations of PSPs in the EU. This will have the benefit of reducing any uncertainty and regulatory arbitrage between national legislation of Member States.

Key Objectives of the PSD3 and PSR

The new payment package aims to address the following objectives:

(1) strengthen user protection and confidence in payments;

(2) improve the competitiveness of open banking services;

(3) improve enforcement and implementation in Member States; and

(4) improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs.

In the following, we consider each of these objectives in more detail, focusing on the core novelties of the proposed legal regime.

2 A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) - Publications Office of the EU (europa.eu)

A closer look at the rules aiming to fulfil the objectives of PSD3 and the PSR

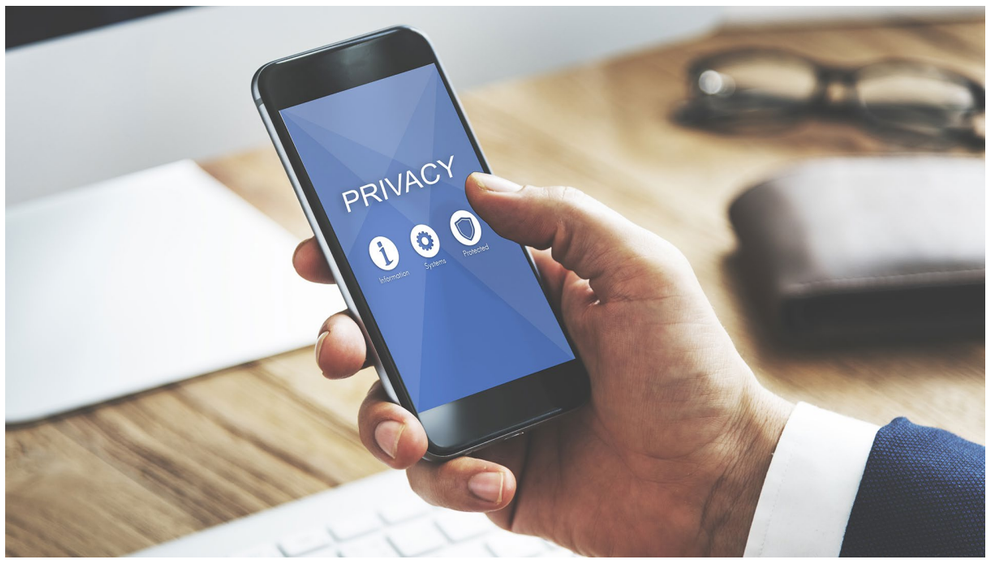
Strengthen user protection and confidence in payments

To strengthen user protection and confidence in digital payments, the EU Commission wants to further improve the application and use of SCA and address the different types of emerging frauds, such as "spoofing" (which is when a perpetrator falsely presents themselves as, for example, an employee of a PSP and utilises such position to commit a fraud).

In case of a fraudulent action, for example spoofing, a PSP will under the PSR be obligated to reimburse the amount transferred due to the fraud, provided however that the user promptly reports the incident to the police and notifies the PSP.[3]

The PSR also provides clarity regarding the scope and usage of SCA[4], including for example in relation to virtual payment cards in mobile wallets.[5] In this regard, a PSP will be required to enter into an outsourcing agreement with its technical service provider if such provider is supplying and verifying the elements of the SCA.[6] It is hence likely that card issuers are required to enter into such outsourcing agreements with providers of digital wallets, such as Google Pay and Apple Pay. Additionally, provisions regarding accessibility requirements have been included in the PSR, ensuring that a variety of SCA methods are made accessible for all types of users.[7] This because the performance of SCA shall not be dependent on the use of a single mean, for example a smartphone.

3 PSR, Article 59.
4 PSR, Article 85.
5 PSR, Recital 118-119.
6 PSR, Article 87.
7 PSR, Article 88 and Recital 110.



Improve competitiveness of open banking services

The emerging need and use of open banking services has created a requirement for a uniform standard of interfaces within the payment industry. In this regard, the PSR sets out obligations for account servicing PSPs (ASPSPs), such as banks, for facilitating their interactions with providers of open banking services. For the purpose of strengthening the interoperability and standardisation between the ASPSPs and the open banking services, the PSR will set out mandatory minimum requirements for application program interfaces (APIs). These shall for instance ensure that payment initiation service providers are able to place and revoke a standing payment order or a direct debit, initiate a single payment and to initiate and revoke a future dated payment.

The PSR also introduces new performance requirements for APIs. These include a requirement for ASPSPs to ensure that their dedicated interface offers at least the same level of availability and performance as the interfaces made available to a user for directly accessing its payment account online.[8] Furthermore, ASPSPs offering payment accounts that are accessible online will also be required to provide a dashboard for monitoring and managing the permissions that the user has given, including allowing the user to manage and withdraw permissions for open banking providers from gaining access to their data.[9]

Improve enforcement and implementation in Member States

One ambition with the proposed PSD3 is to integrate the licensing regimes for PIs and Electronic Money Institutions (EMIs). PIs and EMIs which have already been granted and possess a relevant license, will be required to undergo a re-application process in order to continue to provide payment services or issuing e-money as PIs.[10] Within 24 months of the PSD3 coming into effect, an already licensed PI or EMI would hence have to submit a new application to the competent authority for such authority to assess whether it complies with the new framework and, where it does not, which measures the institution must take to ensure compliance (but also whether the existing authorisation should be withdrawn).[11] There is also an option for Member States to provide for a possibility for automatic re-authorisation.

Although the reasons behind the re-application process are motivated (i.e., to ensure that all institutions operating in the market have been subject to the same harmonised application process), we believe there may be a risk that such re-application process will be costly and may require extensive resources from the applicant. As we see it, specific measures should therefore be taken in this regard to ensure that the re-application process for such institutions will not be unnecessary time consuming or costly. To ensure a harmonised process for the granting of licenses under any such re-application processes, it may also be appropriate to impose to competent authorities a time limit

8 PSR, Article 35 and 37.
9 PSR, Article 43.
10 PSD3, Article 44 and 45.
11 PSD3, Article 44.

for the authorisation process to be concluded, after the receipt of all the information required for the decision.

Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs

The overall purpose of the PSR is to achieve a more even playing field between banks and non-bank PSPs. Under the PSD2, an obstacle for non-bank PSPs has been their inability to gain direct access to certain payment systems, which has resulted in uneven conditions for non-bank PSPs when operating in the market, thus affecting and obstructing the overall competition between service providers.

PSPs need access to payment systems to provide payment services to users. To ensure equal treatment throughout the Union between the different categories of authorised PSPs, the EU Commission has deemed it necessary to clarify the rules concerning access to payment systems (direct as well as indirect via another participant in that payment system).[12] PSD3 thus amends the EU Settlement Finality Directive (SFD) to allow non-bank PSPs to be direct participants in SFD-designated payment systems.[13] As a result, non-bank PSPs would not need to rely on banks in order to execute payment transactions through such systems.

The Commission has deemed that such access should be subject to requirements that ensure integrity and stability of those payment systems, and the payment system operator should hence carry out a risk assessment of a PSP applying for direct participation,

12 PSR, Recital 34.

13 PSD3, Article 46.

including conducting a risk assessment to examine relevant risks (e.g., settlement risks, operational risks, credit risk, liquidity risk and business risks). In this regard, payment system operators should only reject an application for direct participation by a PSP if the payment service provider is unable to respect the rules of the system or poses an unacceptably high level of risk.[14]

Ending remarks

The proposed content of the PSD3 and PSR indicate that there will be a promising transformation in the digital payment landscape within the Union. With a focus on strengthening user protection, conforming license application processes, and expanding access for non-bank PSPs to payment systems, these frameworks set out a solid foundation for creating a more secure, competitive, and innovative payment and financial landscape. However, while these proposals aim to establish and bring significant advantages and clarity for actors in the payment market, their success will, as we see it, be dependent on a balanced and fine-tuned approach being met between consumer protection (including safeguarding security) and the fostering of competition between bank- and non-bank-PSPs. In this regard, we hence see that collaboration and close dialogues are needed between regulatory bodies, financial institutions, and PSPs to ensure a seamless transition into this new regulatory framework, requiring profound involvement from all actors operating in the market.

14 PSR, Recital 34 and Article 31.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Filip Liljekvist
ASSOCIATE
STOCKHOLM

Tokenization of Financial Instruments: The Future of Finance?

Crypto-assets are one of the main applications of distributed ledger technology (in this article, we will use the simplified term "blockchain") in the financial sector. The so-called "tokenization" of financial instruments can be defined as the digital representation of financial instruments on blockchains or the issuance of traditional asset classes in tokenized form to enable them to be issued, stored and transferred on a blockchain. The legal development in this area will have a major impact on the future market. In this article, we examine tokenization of financial instruments with a focus on company shares. Our aim is to bring the reader an overview of the legal aspects and provide an outlook on future legislation.

Tokenization in blockchain: Reinventing an old concept using new technology

In the context of property rights, tokenization is the process of "replacing" a physical or digital asset or right by a token –making the token a *representation* of the asset or right. Ownership or other property rights would typically either be claimed by the holder of the token or by another person or entity noted in a register. In terms of Swedish property law, generally such claimant would likely stipulate strong evidence of being the owner or rightsholder of the asset or right – depending on the applicable legal framework.

The type of tokenization we will focus on in this article is **tokenization in a blockchain context** and its applications for the financial industry. Although this kind of "tokenization" has become a recent buzzword, the act of letting an object represent or symbolize another - thus providing strong evidence for property rights - is in actual fact nothing new at all. Without wandering too far into the annals of Swedish property law, or indeed

creditor protection concepts and the Swedish doctrine of *traditio*, etc., we'll provide a few high-level examples, which are very common in our day-to-day lives:

- Legally speaking, a **promissory note** (*sw*. skuldebrev) is a document (physical or digital) representing the right to collect a debt and receive (future) payment.
- In terms of **real property**, registration in the land registry provides strong evidence of ownership, even stronger if combined with an agreement stating the purchase of the real property (i.e., the contract of sale (*sw*. köpekontrakt), and/or the bill of sale (*sw*. köpebrev)).
- Financial instruments in the form of company **shares** represents a unit of ownership interest in a company as well as stockholder voting rights on matters that affect the company. According to Swedish corporate law, the ownership of a company share is (generally) represented by registration (a note) in the company's share register (*sw*. aktiebok). The purpose of the share register is to constitute a basis for exercise of shareholders' rights vis-à-vis the company; and to provide the company, shareholders and others with information in order to assess the ownership structure of the company. Additionally, any holder of a physical share certificate (*sw*. aktiebrev) is presumed to have a strong claim of being the rightful owner of the share(s), i.e., representing (a fractionalized) ownership of a company.

Utilizing blockchain technology in the financial sector: Use cases

So, what is then tokenization in the context of blockchain and how does it differ from the above?

The blockchain use cases have evolved from the blockchain being solely a facilitator of cryptocurrency transactions - to the emergence of market platforms for trading and issuance of different kind of tokens. This development is providing for enhanced utilization of blockchain in the finance sector and for fintech-solutions.

Using company shares as an example, at least two types of tokenization is emerging on the European market;

1. Utilizing blockchain as the underlying technology for a company's share register, making it possible to (i) issue the share certificate as a token, or (ii) let the share certificate be represented by a token, facilitating the transfer of the share certificate upon change of ownership; and
2. Where the share itself is issued as a token on a blockchain, facilitating the transfer of the share upon change of ownership.

The commonality between the two different types of tokenization related to shares described above is that both types utilize the blockchain as a recordkeeper of the ownership of the company. However, in the context of law, there are a number of differences to be aware of.

Legal aspects of "share ledgers" and tokenized share certificates

Under Swedish law, a company's share register may be maintained using automated processing. Thus, there is no obstacle from a perspective of corporate law of using blockchain as the underlying technology as the "share ledger".

As regards digital copies of, or tokenized share certificates, the legal aspects give rise to a number of issues. Firstly, the Swedish Companies Act[1] prohibits issuance of digital share certificates (*see* chapter 6 para. 3). This means that a share certificate issued by a company in the form of a token would be invalid. And secondly, digital copies or representations of a share certificate in the form of a token would on the one hand indicate ownership of the share, but the current paper-based system for share certificates raises problems in terms of "evidence". A physical share certificate may thus trump its "(non)-equal" of a tokenized share certificate.

Legal aspects of tokenized shares

While Swedish legislation is rather low-key on the notion of tokenized shares, a lot is happening in this area of law in other parts of Europe – introducing legislation streamlined for tokenized assets. For example, Liechtenstein's "Blockchain Act", providing for the tokenization of "everything", took effect in January 2020.[2] Switzerland introduced the concept of tokenized securities by passing its respective act which entered into force in August 2021.[3]

On the EU side, there is a vast legislative work in progress in order to regulate the crypto market, introducing, e.g., the Markets in Crypto-Assets Regulation[4] (the "MiCA-

1 The Companies Act (SFS (Swedish Code of Statutes) 2005:551).
2 The Token and Trusted Technology Service Provider Act (TVTG).
3 The Federal Act on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology and the associated blanket ordinance.
4 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

regulation") and the DLT Pilot Regime (as defined below).[5] The MiCA-regulation creates clarity on the notion of tokenized financial instruments by actively bringing it outside its scope; instead referring to well-established EU regulatory frameworks for the financial sector, e.g., the Markets in Financial Instruments Directive (MiFID II).[6]

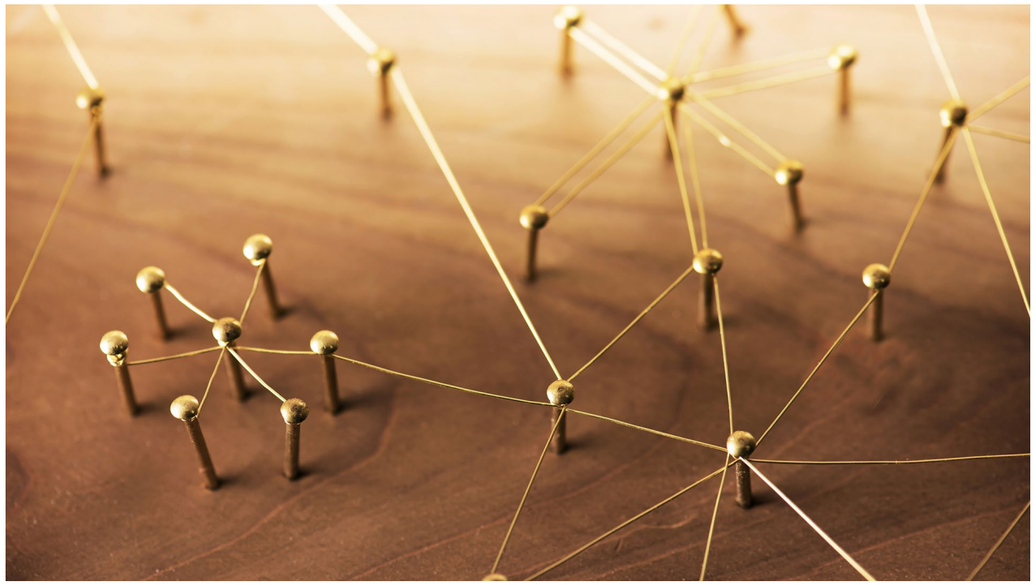
The regulatory sandbox: An insight into future legislation

Another "legislative project" from the EU is the DLT Pilot Regime[7] which introduces a union-wide legislation which provides the opportunity of operating DLT market infrastructures subject to temporary exemption from some specific requirements of EU financial services legislation. The overall goal of letting players in the market operate "freely" is for the purpose of testing and letting the EU legislators gain valuable experience regarding tokenized financial instruments and their underlying technologies. The aim is to develop the trading and settlement for tokenized financial instruments and insights to be gained are supposed to be helpful in the identification of possible practical proposals for appropriate regulatory frameworks. The focus is on regulatory proposals for the issuance, safekeeping and asset servicing, trading, and settlement of tokenized

5 Setterwalls examines the MiCA-regulation in several articles. For more information, see: https://setterwalls.se/en/article/the-mica-regulation-ten-steps-for-crypto-companies-to-consider/ and https://setterwalls.se/en/article/the-upcoming-eu-crypto-asset-regulation-mica-are-nfts-to-be-regulated-like-crypto/ and https://setterwalls.se/en/article/the-new-eu-crypto-asset-legislation-mica-are-the-wild-west-days-of-crypto-about-to-end/

6 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

7 The "DLT Pilot Regime": regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology entered into force on 23 March 2023. The DLT Pilot Regime is part of the EU Digital Finance Package, among the MiCA Regulation and the Digital Operations Resilience Act.



financial instruments.[8]

Three types of "DLT market infrastructures" are introduced by the DLT Pilot Regime (somewhat simplified in the below description):

- *DLT multilateral trading facilities* ("DLT MTFs"): multilateral systems operated by an investment firm or market operator approved under MiFID II — which only admits to trading tokenized financial instruments.
- *DLT settlement systems* ("DLT SS"): a system that settles transactions in tokenized financial instruments against payment or against delivery and that allows the initial recording of or the provision of safekeeping services in relation to tokenized financial instruments.
- *DLT trading and settlement systems* ("DLT TSS"): a DLT MTF or DLT SS that combines services performed by a DLT MTF and a DLT SS.

Furthermore, the specific kind of tokenized financial instruments which are enumerated in the regulation are (i) shares, (ii) bonds, and (iii) units in collective investment undertakings.

The European Securities and Markets Authority ("ESMA") is responsible for providing a report to the EU Commission on 26 March 2026, stemming from this Pilot Regime-project evaluating a number of different aspects. The ESMA report shall serve as a basis for the final evaluation report to be presented by the EU Commission to the European

8 Setterwalls examines the DLT Pilot Regime in this article: https://setterwalls.se/artikel/blockchain-regulation-in-the-spotlight-key-takeaways-from-the-eu-dlt-pilot-regime/.

Parliament and the Council. This final report shall include a cost-benefit analysis on whether the Pilot Regime should be extended, if it should also include other kinds of financial instruments, or whether it should generally be amended, be made permanent or be terminated. ESMA will also provide interim reports annually in order to, e.g., provide the market participants with information on the functioning of the markets, address incorrect behavior of operators of DLT market infrastructures, provide clarifications on the application of the regulation and update previous indications based on the evolution of blockchain technology.

Are tokenized financial instruments the future of finance?

One thing is for sure, and that is that entrepreneurs and companies are eager to follow the legislative development in the EU – as future legislation forms the framework for

Emily Svedberg-Possfelt
SENIOR ASSOCIATE
GOTHENBURG

Hanna Lindqvist
ASSOCIATE
GOTHENBURG

Consumer terms in the cryptocurrency market – the Swedish Consumer Agency's review and conclusions of crypto-asset intermediaries' terms and conditions

In a memorandum from 19 June 2023, the SCA revealed its hand on what it considers to be unfair standard terms for a cryptocurrency asset intermediary, which is active in the Swedish market. The memorandum serves as a 22-page-long consumer and marketing compliance checklist, which should be closely studied by any intermediary who aims to precede the SCA before its scheduled follow-up review in 2024.

Background

Looking back over the past year, the cryptocurrency industry has been quite volatile with the bankruptcy of FTX Trading Ltd, and an investment climate which favours more traditional, 'safe' assets. That being said, some green shoots can be discerned. One such green shoot is Coinbase's recent approval to offer American customers the option to trade cryptocurrency futures, effectively allowing cryptocurrency assets into the "futures club", alongside other pristine members such as wheat, oil, and the S&P 500.

In Sweden, as well as throughout most of Europe; the cryptocurrency landscape is not short of interesting developments, such as the new upcoming EU Crypto Assets Regulation.[1] On a national level, the Swedish Consumer Agency (the "SCA") recently released a memorandum,[2] covering its findings after having reviewed the terms and conditions of several cryptocurrency asset intermediaries operating in Sweden. In the memorandum, the SCA accounts for various clauses which will require every cryptocurrency asset intermediary's attention before the SCA's follow-up review, scheduled in 2024.

In this article, we will take a closer look at the SCA's memorandum[3], what insights it has to offer, and which actions will be needed by the intermediaries before the SCA's scheduled follow-up review.

The CCA

In Sweden, there are currently no specific laws regulating the marketing of cryptocurrency assets. Instead, cryptocurrency asset intermediaries are subject to the general rules of inter alia the Marketing Act (2008:486, Sw. Marknadsföringslagen), the Price Information Act (2004:347, Sw. Prisinformationslagen) and the Consumer Contracts Act (1994:1512, Sw. Lag om avtalsvillkor i konsumentförhållanden "CCA").

Under the CCA, the Patent and Market Court ("PMC") may prohibit a trader from using a specific contractual clause, if the clause is deemed unfair to the consumer and the prohibition is justified from a public perspective or otherwise serves the interest of consumers or competitors. A prohibition by the PMC shall, as a rule, be accompanied with a conditional fine for any non-compliance by the trader, and shall further cover the use of any clauses which are essentially the same as the one prohibited by the PMC.[4] In addition to the PMC, the Consumer Ombudsman may also in some cases issue an injunction calling for a trader to cease with the usage of a certain contractual clause.[5]

What constitutes an "unfair" clause under the CCA is preceded by an overall assessment of the rights and obligations of the parties and can, typically, be divided into three main groups: (i) clauses that contravene mandatory legislation or general legal principles, (ii) clauses that contravene permissive law and where the outcome results in such a significant disadvantage for the consumer that there is no reasonable balance left between the parties, and (iii) clauses that are so misleading or unclear that the consumer is misled in their meaning of the consumer's rights. Other relevant factors for the overall assessment of what constitutes an "unfair" clause are, for an example, the type of service or goods covered by the agreement, or if the clause has been subject to individual negotiation between the parties, or if it constitutes so-called "standard terms".

In order to extract the legislators' intention over what constitutes an "unfair" clause, one must closely study the available case law. In addition to relevant case law, further guidance can also be sought in the so called "grey list"[6], which contains a set of clauses which are typically considered unfair. However, it should be noted that the list is both

1 In the 2022 issue of Setterwalls FinTech Report, we discussed the new upcoming EU Crypto Assets Regulation ("**MiCA**"). For more information regarding the upcoming MiCA regulation, please be referred to *The Upcoming EU Crypto Asset Regulation (MiCA) – are NFTs to be regulated like crypto?* Available here.

2 The memorandum is available in Swedish and can be read here.
3 In the memorandum, the SCA also reviews the cryptocurrency asset intermediaries marketing activities. However, in this article we will only be discussing the SCA's review of the contractual clauses.
4 Section 3 of the CCA.
5 Section 7 of the CCA.
6 The "grey list" is an appendix to directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, which implementation led to the CCA. In Sweden, the appendix was not included in the CCA, why the "grey list" can either be found in the legislative history of the CCA, alternatively in the appendix to the directive 93/13.

non-binding and non-exhaustive, meaning that other types of clauses, other than the ones mentioned, can also be considered unfair (and, of course, vice versa).

Contractual Clauses Questioned by the SCA

In its memorandum, the SCA mainly focuses on clauses relating to, jurisdiction, arbitration, class action, requirements for written termination, notices of change in terms and conditions, and disclaimers.[7] In the following, we will discuss the SCA's reasoning and share our view as to what can be considered 'best practice' after the memorandum.

Jurisdiction, Arbitration and Class Action

Regarding clauses relating to jurisdiction, arbitration, and class action, the SCA refers to the grey list and states that terms which excludes or hinders the consumer's right to take legal action or exercise any other legal remedies, typically are to be considered unfair. In particular, this includes terms which state that any dispute between the trader and the consumer shall be settled by arbitration, or where the consumer is unduly restricted to evidence that should typically be available to the consumer, or otherwise if the consumer is imposed with a burden of proof which by law should lie with the cryptocurrency asset intermediary.[8]

The SCA's standpoint regarding jurisdiction, arbitration and class action clauses aligns with standard market practice. Therefore, cryptocurrency asset intermediaries should ensure the formulation of, or otherwise amend, their terms in accordance with the views expressed in the memorandum.

Requirements for Written Termination

One of the more interesting standard clauses which the SCA discusses is the requirement for written termination. In its memorandum, the SCA points out that several cryptocurrency asset intermediaries include terms through which the consumer is imposed with requirements to terminate the agreement in writing, and that such requirements are to be considered unfair under Article 3 of the CCA, following applicable case law. The statement should not be interpreted as a general prohibition for an intermediary to impose terms regarding written termination, but rather that it is not allowed to only offer the consumer the option of terminating an agreement in writing.

A consumer's utilization of a cryptocurrency asset intermediary's services may involve assets which can amount to a considerable sum. Arguably, a safe, easy, and accessible option for consumers to terminate their agreement with the intermediary would be by offering an online termination option through the consumer's account, which is nearly considered standard practice these days. However, according to the SCA, an intermediary which exclusively offers this way of termination, is in breach with Article 3 of the CCA. Instead, in order to be compliant, the intermediary must also offer alternative methods for termination. Other termination methods might include contacting the intermediary by phone call or visiting their local offices. In our view, it could be questioned whether such options in practice actually makes any difference, given that the average Swedish

7 In its memorandum, the SCA also review *cryptocurrency asset intermediaries' liability for information published on its website*. However, since the review in that regard is mainly conducted from a marketing perspective, and under the Marketing Act, it will not be discussed in any further detail in this article.
8 Section 1 (q) of the grey list.

consumer is generally very familiar with using the internet and availing of digital tools.

It should be noted that terms which stipulate a requirement for written termination are not formally included in the grey list, meaning that there is no assumption that such a requirement is to be considered unfair. Instead, case law ultimately determines whether the clause can stand or fall. Regardless of the SCA's standpoint regarding written termination, we hope that future case law will address and clarify whether providing alternative termination methods truly serves the consumer's best interests or merely imposes unnecessary and burdensome regulations on intermediaries.

Notices of Change in Terms and Conditions

Another interesting and notable aspect relates to how terms may be changed. In its memorandum, the SCA concludes that several intermediaries reserve the right to alter the terms at any time, at their own discretion, and without any obligation to notify consumers about the changes. Additionally, the consumers are referred to the intermediaries' websites, where they can access the latest version of the terms and conditions.

Clauses which give the trader the right to unilaterally alter the terms and conditions are included in the grey list and are typically considered unfair.[9] However, the grey list exempts suppliers of financial services, effectively allowing them to unilaterally alter the terms in an ongoing agreement without a valid reason, provided that the supplier informs the consumer with reasonable notice and that the consumer is free to dissolve the

9 Section 1 (j) of the grey list.

contract.[10] In its memorandum, the SCA states that services offered by a cryptocurrency asset intermediary does not formally qualify as a financial service. However, the SCA argues that the intermediary's services should analogously qualify as a financial service, whereas the exemption in the grey list is applicable.

More interestingly, the SCA also discusses terms through which the intermediary is allowed to unilaterally add or withdraw various cryptocurrency assets (or adjust trading volumes), without any obligation to inform the consumer about such changes. According to the SCA, any change in the intermediary's offering is to be considered an amendment to the terms and should be treated like other alterations. However, we believe that there is a distinction between adding and withdrawing cryptocurrency assets from an intermediary's platform. For an example, when cryptocurrency assets are withdrawn from the platform, it can significantly impact the consumer's investment strategy or disposition of its assets. Because of these potential implications, we assert that any changes which include the withdrawal of cryptocurrency assets should be accompanied by reasonable notice. On the other hand, considering that the same implications do not occur when an intermediary is adding assets to its platform, it could likewise be questioned as to whether the same principle should apply, and whether the action necessitates the intermediary to notify the consumer of a change in the terms.

10 Section 2 (b) Paragraph 2 of the grey list.

Disclaimers

In its review of disclaimer clauses, the SCA refers to the legislative history of the CCA and states that terms which contradict mandatory general legal principles – even if such principles are not explicitly stated through law – are prohibited. Here, the SCA illustrates its point and refers to terms where a trader exempts itself from liability in cases of gross negligence, or when a trader applies terms with the intention of circumventing mandatory legal provisions.

To summarise, the SCA primarily objects to two types of disclaimers. The first type includes sweeping disclaimers that, in practice, covers all situations where a consumer has suffered damages, regardless of the cause, including situations resulting from the trader's negligence. The second type of disclaimer involves traders capping the amount of compensation consumers can receive for damages caused by the trader. In reference to the second type, the SCA cites the case of MD 2002:23. In this case, the trader had an annual liability cap of SEK 10,000, intended to cover all damages. The court determined that this cap restricted the trader's liability, even when general principles would require higher compensation than SEK 10,000. Therefore, the cap was deemed to be unfair according to Section 1(b) of the grey list.

In our opinion, one could question whether MD 2002:23 should be interpreted as a general prohibition against liability caps. For instance, Section 1 (b) of the grey list states that terms which "inappropriately" exclude or limit the legal rights of the consumer towards the trader, in the event of total or partial non-performance or inadequate performance by the trader, may be regarded as unfair.[11] Based on the wording of Section 1 (b) of the grey list and, by extension, the court's ruling, liability caps that are appropriate could potentially be considered reasonable and thus allowed. What constitutes such an appropriate liability cap remains unclear. However, an informed conjecture would be that the amount of the liability cap, in conjunction with the specific nature of the trader's business, is highly relevant in making this determination.

11 Again, it should be noted that the grey list solely holds a guiding, non-binding, position in Swedish law.

Summary

As of today, there are no specific laws regulating the marketing of cryptocurrency assets. Therefore, inter alia, the CCA must be consulted when reviewing a cryptocurrency asset intermediaries' terms and conditions. In simplified terms, a term which is deemed unfair under the CCA may be prohibited by the PMC if this is justified from a public perspective or otherwise serves the interest of consumers or competitors. The determination of what qualifies as an "unfair" term involves an overall assessment, with the grey list serving as important interpretative data.

Our general assessment is that the SCA's memorandum – in most cases – accurately reflects applicable law and serves as a helpful "checklist" for the actions which an intermediary must undertake before the scheduled follow-up review in 2024. However, in our view, the SCA's conclusions can to some extent be probed further, especially regarding requirements for written termination, notices of change in terms and conditions and disclaimers. Here, additional assessments must be made individually, on a case-by-case basis. In this regard, we therefore welcome additional case law which will ultimately help to shed light on these questions and concerns, which emanate from the current lack of clarity.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Joel Kokko
ASSOCIATE
STOCKHOLM

Building a strong foundation: how legal best supports first line operations for business success - interview with Qliro

It can be challenging for a company in the FinTech sector to adapt to new legal frameworks. In recent years, besides a few national initiatives, the EU has introduced a number of regulations and directives affecting regulated companies and actors in the FinTech sphere. Financial companies are required not only to field a substantial legal and compliance department, but also often needs to involve external expertise and consultants to ensure that the business meets all legal requirements that are imposed on it.

Efficient and streamlined business operations, including skilled employees, efficient marketing efforts etc. are all fundamental for a successful business. Yet, legal and compliance may in certain aspects be *just as,* or even more, critical. In this article, we delve into how the integration of legal support and proactive legal compliance can bolster the first line operations of FinTech companies to contribute to the success of business and share how FinTech company Qliro has worked to achieve their goals in this regard.

The Role of Legal in First-Line Operations

The first line operations are at heart of a financial company's business; the day-to-day production and sales of the services or goods provided, directly interacting with customers and suppliers. Well-oiled first line operations are fundamental for a business to succeed. But without the integration of a sound legal foundation, even the greatest business operations can falter.

FinTech companies are also, just like traditional financial institutions, vulnerable to different types of legal risks and uncertainties. Failing to understand the legal risks, which may be unique to the specific business, may for example lead to unexpected, and almost always unnecessary, legal disputes with suppliers and or authorities.

For businesses operating within industries with strict regulations, such as financial markets, legal compliance is not just good practice, but the bedrock which the business itself must be built upon.

Proactive legal compliance

In the fast-paced world of FinTech, businesses must quickly adapt to the everchanging regulatory landscape, and consider new business lines and opportunities in light of applicable regulations.

We have had the opportunity to interview Carin Eriksson, Head of Legal at Qliro. Qliro, headquartered in Stockholm, was founded in 2014 and is a fast-growing FinTech and licensed credit-market company (Sw. *kreditmarknadsbolag*) offering safe and simple digital payment solutions for e-commerce. Carin joined Qliro as Head of Legal in 2022. Carin's background is within banking and finance, and she has spent several years at a larger Nordic law firm. She has also been a part of the in-house legal team at one of the largest banks in the Nordic region.

The legal team of Qliro works closely with their colleagues in other departments to ensure that Qliro is not only compliant with existing regulations but also aware of how and why certain actions and steps are required of them in their daily work. Such cooperation also enables Qliro's legal team to better understand the impact of a particular legislative change, or the introduction of a new law, on the company's day-to-day operations.

During the interview, Setterwalls sat down with Carin and discussed the challenges and opportunities related to the introduction of new laws and regulations, and how legal can support the business to adapt to the entailing changes.

For some insights into this, below is a summary of our interview with Carin:

Q: Could you please provide a brief overview of Qliro and its position within the FinTech field?

Qliro is a Swedish FinTech listed on Nasdaq Stockholm. Qliro is authorized by the Swedish Financial Supervisory Authority (*Sw. Finansinspektionen*) as a credit-market company. Our business, and our products, are two-folded, as we offer payment solutions to both e-commerce companies (B2B) and consumers (B2C). Our offering to our B2B clients includes a safe and simple all-in-one checkout and the offering to our B2C clients includes *Buy-Now-Pay-Later* and more traditional credit solutions. We also offer various direct payment methods through our payment partners in the Qliro checkout.

We work every day to make the purchase experience as safe and simple as possible for both merchants and consumers.

Q: How has Qliro integrated its legal department into its first-line operations?

As a listed and regulated company, legal compliance is of utmost importance for the operations we conduct. There are rules impacting almost all parts of our business.

It has therefore been an important process and a priority for us, which we are continuously working on, to spread knowledge within the company and ensure that all

our employees are aware of and understand the requirements we have as a listed credit market company. Even though we are a relatively small player, the regulatory landscape is mostly the same as for bigger companies.

Recognizing the significance of legal compliance is typically a challenge for any organization. Early involvement of legal expertise in the company's strategic projects and initiatives, on one hand, and a solid business understanding within the legal team on the other, are key to ensure alignment between internal stakeholders, as well as seamless cooperation in regulatory matters.

Q: Could you give us an example of how legal is involved in the preparation of a new product or service?

When for instance developing a new product or changing a product, the legal team's involvement is required at several stages of the product development process. This process then requires that we have a good understanding of the legal requirements for such a product and that we (*i.e.,* Qliro's legal department) thus assist our product development teams in its development.

On a concrete level, taking a consumer credit product as an example case, such assistance can be to help the product managers to understand what type of fees and interest we are allowed to charge and how it should be structured, or what type of consumer protection measures must be in place, and so forth.

We also need to work closely with our IT and data engineers to design the digital product offering to ensure legal compliance. Our product offering is hence subject to continuous iteration and cooperation between several departments within the company, whereby legal is one of the key stakeholders.

Q: What are the main challenges you and your team face and how do you cooperate with external experts?

It is an ongoing process to keep up to date with new legislation, especially as we operate in several markets and countries in the Nordic region.

In certain instances we also use external law firms, for example where we may not have the right skills ourselves, or if we have a major project where we may need external support to be able to effectively bring it to completion. It is important that our partners and advisors are familiar with our activities and the business itself, in order for us to fully benefit from their support. It is key that the advisor understands what is of key importance to the project and the business, and that they fully grasp our needs, in order to make our collaboration successful.

Q: How do you and your team ensure that the first-line operations teams stay informed about regulatory updates, and describe your approach to working with them?

As mentioned earlier, our role is to be a sounding board for Qliro's operations, informing our colleagues about news and regulatory changes, how they affect our business and how we need to adapt. But it is also important that we are able to speak up and that we are allowed to be a part of the business and product development that one might otherwise think the legal team is not usually part of.

The legal team also works to constantly compile, update, and keep records of which laws and guidelines apply to our business and our services, which of course depends on the jurisdiction we operate in, and the respective service we are providing to our customers.

It is not always the case that a new major act or law will automatically have the greatest impact on the business side of our operations. Also legal changes which at an initial stage are deemed to be of minor magnitude can, eventually, force the business to take rather extensive integration measures. There is therefore always a need to analyse all new legislations, as the same compliance requirements are often imposed on the smaller FinTech operators just as much as they apply to the larger ones.

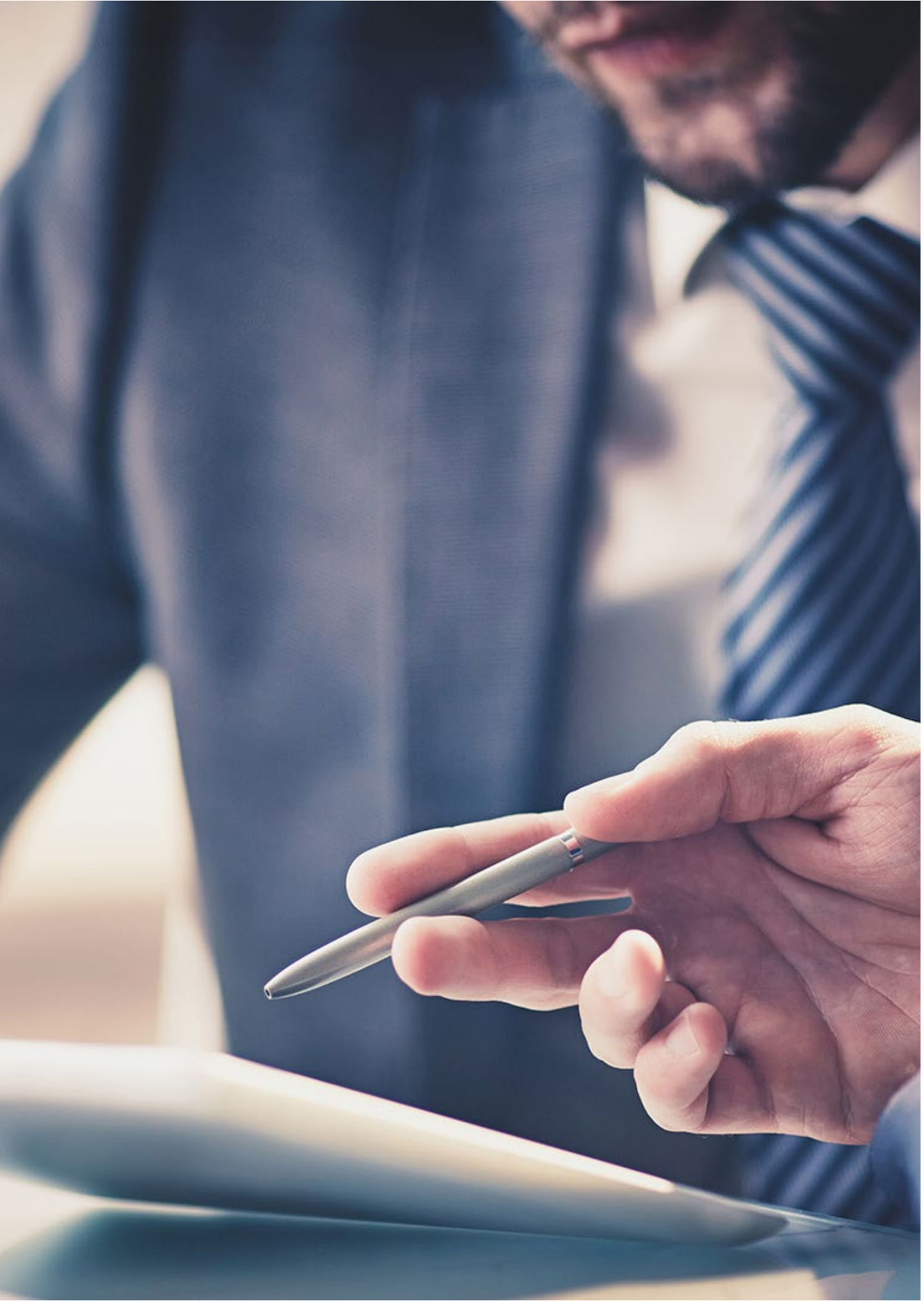
To conclude

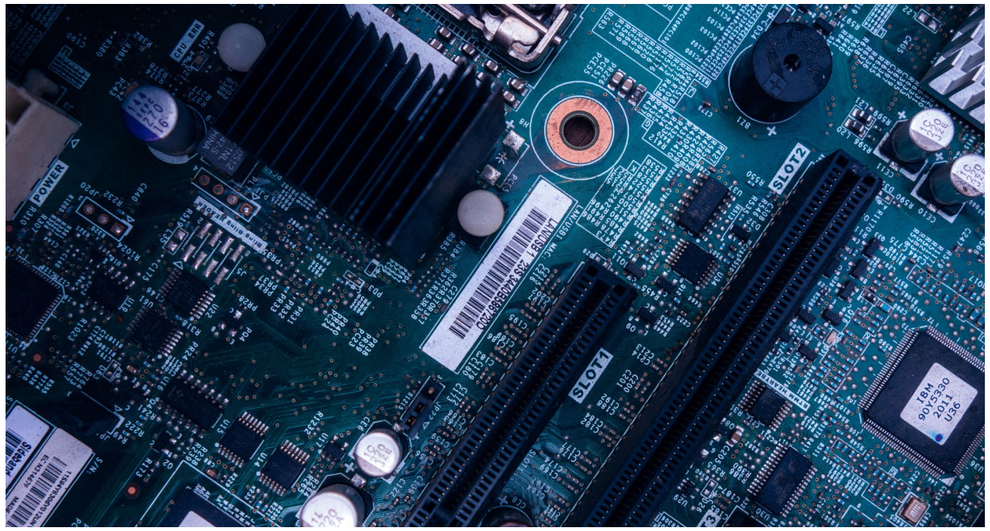
Navigating the ever-evolving legal landscape of FinTech, and the legal framework's profound impact on the financial industry, presents both challenges and opportunities for its stakeholders. A sound understanding of legal compliance for the operations of FinTech companies has never been more important than it is today. The delicate balance between innovation, regulation, and legal compliance is paramount in shaping the future of FinTech.

Thank you Carin, and the Qliro legal team for your valuable perspective.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Rasmus Lindholm
ASSOCIATE
STOCKHOLM





Unraveling DORA: Cyber Resilience Requirements in Digital Finance

In the fast-moving and ever-evolving world of digital finance; data protection and cybersecurity are not merely buzzwords, but fundamental prerequisites for operational success. The European Union ("EU") recognizes this reality, and the Digital Operational Resilience Act ("DORA") is an EU regulatory response that came into force in January 2023. Designed specifically to address the unique needs and challenges of the financial sector, DORA has the potential to reshape the cybersecurity landscape for financial institutions across Europe. In this article, we unravel the key aspects of DORA, its implications, and how it may revolutionize data protection and operational resilience within the financial industry.

The Essence of DORA for Finance

DORA is part of the EU's sweeping initiative to modernize the regulatory framework for the digital sector, with a primary focus on financial institutions. Here are the core objectives that DORA aims to accomplish:

Fortifying Operational Resilience: In a financial world driven by digital technologies, resilience is paramount. DORA seeks to empower financial institutions to withstand cyber-attacks and operational disruptions, ensuring business continuity and safeguarding financial services. DORA necessitates the implementation of robust risk management and incident response frameworks. Financial institutions will be required to conduct thorough risk assessments, take preventive measures, and establish efficient protocols

for responding to cyber incidents.

Streamlining Reporting: Financial entities often deal with complex reporting obligations in the event of cyber incidents. DORA promises to streamline this process, making it more consistent and easier to navigate for financial firms. This minimizes operational disruptions and facilitates more effective regulatory oversight.

Empowering Oversight: DORA grants supervisory authorities increased authority to both set and monitor cybersecurity standards for financial institutions. This represents a pivotal shift towards a more controlled and secure financial ecosystem.

Data Protection: Data is the lifeblood of the financial industry. DORA takes data protection seriously, ensuring that financial institutions comply with the highest standards to secure client data and maintain GDPR compliance.

Key Provisions Tailored for Finance

DORA includes provisions tailored specifically for financial institutions, making it a comprehensive and industry-specific regulatory instrument. Recognizing the unique challenges of the financial industry, DORA encompasses a broad range of financial entities, including banks, insurance companies, payment service providers, and trading platforms.

In order to achieve a high level of common digital operational resilience, DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(a) requirements applicable to financial entities in relation to:
  (i) information and communication technology (ICT) risk management;
  (ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the authorities;
  (iii) reporting of major operational or security payment-related incidents to the authorities (applies to credit institutions, payments institutions, account information service providers and electronic money institutions);
  (iv) digital operational resilience testing - including testing in cooperation with critical service providers to the entity;
  (v) information and intelligence sharing in relation to cyber threats and vulnerabilities;
  (vi) measures for the sound management of ICT third-party risk;

(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) rules for the establishment and conduct of an "Oversight Framework" which will, e.g., develop technical standards and supervise and scrutinize critical ICT third-party service providers when providing services to financial entities;

(d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by DORA. DORA also introduces substantial penalties for non-compliance with its provisions.

Anticipated Impact on Financial Institutions

For financial institutions, DORA holds immense significance. It promises to create a more secure and resilient operating environment, thereby enhancing customer trust, preserving sensitive financial data, and reducing operational risks. The legislation's ripple effects are also expected to resonate globally, influencing cybersecurity and data protection standards beyond the EU's borders.

Furthermore, financial institutions operating in the EU or looking to access the EU market will need to adhere to DORA's requirements. This could drive global harmonization of cybersecurity practices, potentially increasing efficiency and reducing compliance complexities for international financial players.

Conclusion

DORA is not merely a regulatory framework; it's a fundamental shift in how cybersecurity and data protection are approached by the financial sector. By focusing on operational resilience, streamlined reporting, oversight, and data protection, DORA is set to elevate cybersecurity standards for financial institutions across Europe. For those in the financial sector, DORA represents an opportunity to embrace a new era of cyber resilience and data protection, ensuring not just compliance, but also safeguarding the reputation and trustworthiness of financial services. In an industry where data is everything, DORA is a milestone in shaping the future of cybersecurity and data protection.

DORA comes into effect in January 2025, and entities under its scope are recommended to start implementing measures for compliance. Considering that the authorities are issuing complementary guidelines (e.g., regulatory technical standards (RTS) and implementing technical standards (ITS)), we advise entities under its scope to conduct continuous gap-analyses in order to assess and implement all relevant measures needed for complete DORA compliance.

Emily Svedberg-Possfelt
SENIOR ASSOCIATE
GOTHENBURG

Hanna Lindqvist
ASSOCIATE
GOTHENBURG

Open Finance under FIDA – What to Expect from a Swedish Perspective

Digital technologies relying on data are increasingly driving change in the financial industry by providing fintech companies with new business models and ways to engage with customers. In an effort to modernize the current legal framework and to keep up with technical developments, the European Commission has proposed enhanced rules on financial data access (open finance). In this article, we focus on what can be expected from access to a broader set of financial data for a wider range of financial players, based on Swedish conditions.

The predecessor of open finance - the current legal framework for open banking

The second Payment Services Directive (PSD2), adopted in 2015, sets out the rules for payments in the EU with the purpose of ensuring a level playing field between existing financial players and upcoming payment providers. One of the main aims of the PSD2 is to increase competition and facilitate innovation in financial services by opening the EU market for upcoming providers, offering payment services based on access to financial data from payment accounts. This is achieved through the PSD2 forcing account servicing payment service providers (mainly the banks) to open access to their customers' payment accounts data to external parties, so-called third-party providers (TTP), via APIs. These TPP are divided into two types: payment initiation service providers (PISP) and account information service providers (AISP).

While PSD2 has made significant progress in opening and fostering competition and innovation in the EU payment market through open banking, this has not targeted the wider financial sector, and has been limited to financial data from payment accounts. In response to this and following an evaluation of PSD2, the European Commission has put forward a series of proposals. These lay down the framework for the third Payment Services Directive (PSD3), the Payment Services Regulation (PSR) and the regulation on a framework for Financial Data Access (FIDA), fostering the move from open banking to open finance.[1]

Open finance under FIDA

Access to a broader set of financial data for a wider range of financial players

The proposed framework for open finance aims to facilitate the provision of individualised, data-driven products and services that may fit the individual customer's specific needs. It is based on the open banking concept whereby customers have the option, but not the obligation, to enable access to their financial data. However, while PSD2 only applies to payment accounts, FIDA will cover a much wider range of financial data. Based on the principle that the financial data should demonstrate a high value-add for financial innovation, as well as low financial exclusion risk for customers, such data includes:

- mortgages, loans and accounts (other than payment accounts regulated under PSD2);
- savings products, financial instrument investments, crypto assets, real estate and related investments;
- occupational and personal pension products;
- non-life insurance products (excluding sickness and health insurance); and
- data which forms part of a creditworthiness assessment of a firm.[2]

The right to access this wider set of financial data will apply for the following financial institutions:

- credit institutions;
- payment institutions including AISPs;
- e-money institutions;
- investment firms;
- crypto assets service providers;
- issuers of asset-referenced tokens;
- managers of alternative investment funds;
- management companies of undertakings for collective investment in transferrable securities;

1 https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_sv
2 FIDA, Article 2(1).

- insurance and reinsurance undertakings;
- insurance intermediaries and ancillary insurance intermediaries;
- institutions for occupational retirement provision;
- credit rating agencies;
- crowdfunding service providers;
- PEPP providers.[3]

In addition to the above-mentioned financial institutions, FIDA will introduce a new type of authorised entity, the so-called financial information service provider (FISP). FISPs will be allowed to have access to customers' data for the sole purpose of providing financial information services (more on the differences between financial institutions and FISPs below).[4]

Data access obligations

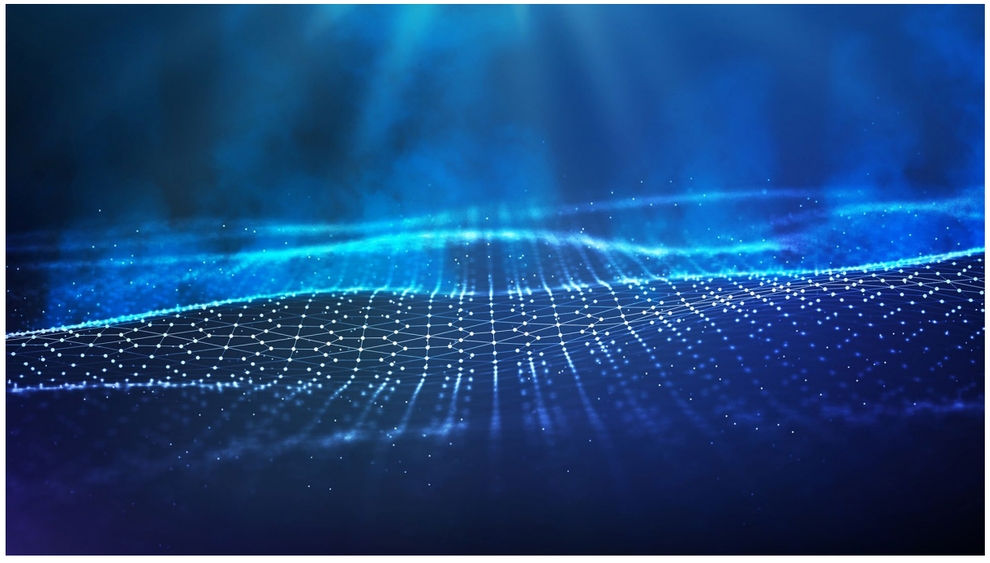
FIDA differentiates between data holders – entities that collect, store and otherwise processes customers' data, and data users – entities that, following the permission of a customer, have lawful access to customer data. Upon customers' request, institutions that act as data holders will be obliged to make customers' data available to them without undue delay and free of charge.[5] The same obligation will apply where request for data access is sent by a data user that acts based on customers consent. However, in this case, financial institutions acting as data holders will be able to receive compensation for this service, which is one of the major differences between FIDA and PSD2.[6]

All financial institutions, except AISPs and FISPs, will generally be able to act as both data holders and data users. Thus, the roles of data holder and data user are not mutually exclusive. For example, an investment firm may be required to share customer data with data users at the request of a customer. But that same investment firm could be authorised by its customers to request data from other data holders, e.g., loan or pension providers, to improve its offerings.

Financial data sharing schemes

Within 18 months from the entry into force of FIDA, data holders and data users will be required to join one or more financial data sharing schemes. The schemes will be responsible for governing access to customer data in compliance with FIDA, and other applicable EU rules (such as the GDPR and the Data Act). Financial data sharing schemes will have to develop common standards for data sharing and interface requests, set member contractual liabilities, and provide effective dispute resolution mechanisms. Financial data sharing schemes will also establish the model to determine the maximum compensation data holders may charge users. [7]

3 Ibid, Article 2(2).
4 FIDA, Preambles 31-34 and Articles 2(2) and 3(7).
5 Ibid, Article 4.
6 Ibid, Article 5.
7 Ibid, Articles 9 and 10.



If no financial data sharing scheme is developed for a category of customer data covered by the FIDA, the European Commission will be empowered to adopt a delegated act to set common standards for data sharing and technical interfaces, a model to determine maximum charges for data sharing and the liability of entities making customer data available.[8]

A number of Swedish-specific factors

In a Setterwalls article from July 4 2023, we focused on the Swedish Financial Supervisory Authority's (the SFSA) report on the use of open financial services in Sweden.[9] In preparation for the upcoming regulations, the SFSA has on behalf of the Swedish government conducted a survey of how these services are used in Sweden, and identified and analysed any risks and opportunities linked to them.[10]

The SFSA's report highlights that Swedish fintech companies have been earlier adopters of open financial services compared to the rest of Europe. This is attributed to the highly digitised financial industry in Sweden, the presence of innovative fintech companies, and the early and extensive use of mobile e-IDs. Amongst the open financial services, payments are one of the most widely used applications, but payment initiations through open financial services have been shadowed by and recently also lost ground to other popular payment services.[11] This may indicate that the Swedish market has reached a

8 Ibid, Article 11.
9 Setterwalls' article from July 4 2023, *Key takeaways from the new SFSA report on open finance in Sweden*.
10 The SFSA Report from June 28 2023, *Användningen av öppna finansiella tjänster i Sverige*.
11 Ibid, p. 7-8.

high level of competition regarding payment initiation services and that FIDA is a much-needed regulation for fintech companies to provide open financial services within financial sectors not limited to payment initiations.

According to the SFSA, the use of open financial services within the insurance sector, although lacking a regulated retrieval method and not widely used at present, shows a rising trend of use in Sweden. Thus, there seems to be a need for regulated open financial services within the insurance sector, but the need for such services depends on the insurance in question. As an example, for non-life insurances and pension insurances, the primary interest is considered to be a good basis for warranting a switch of insurance company. Thus, the current use in these fields tends to be mainly sales-driven, rather than providing the insurance holder with more information and a better overview of their insurances.[12]

Another sector of interest is the savings and investments industry, where the use of open financial services according to the SFSA's report is relatively low. Following dialogue with industry stakeholders, the SFSA notes that Sweden is deemed advanced in the development of pensions and savings transfers, which may be provided through open financial solutions.[13] This industry is thus not currently subject to a high level of use (or perhaps supply) of open financial services and there may be potential for innovation.

12 Ibid, p. 9-10.
13 Ibid, p. 12.

To conclude

The proposed framework for financial data access is a welcome development for innovation within the financial industry, providing new opportunities for both current major financial players, as well as up-and-coming fintech companies. FIDA still needs to find its way through the EU legislative process, which may be prolonged by the upcoming EU election. Nevertheless, due to the complexity of FIDA, financial institutions should use this time wisely, in order to start preparing in advance for ultimate implementation. Setterwalls will continue to closely follow all developments as FIDA goes through the EU legislative process, and will also monitor any further updates from the Swedish government.

Niklas Follin
PARTNER
STOCKHOLM

Hanna Salajin
ASSOCIATE
STOCKHOLM

Generative AI is here – what to consider for companies when using generative AI technology

Introduction

In recent years, artificial intelligence (AI) has generated significant interest and has ignited debates and discussions amongst experts, as well as the general public. For many, AI is a concept of the future and commonly associated with advanced technologies. More recently, AI has become associated with chatbots such as ChatGPT, which is an example of an AI tool falling within the realm of generative AI.

In this report, we take a closer look at generative AI, shedding light on its applications, risks, and potential legal implications. Our goal is to enhance the reader's understanding not only of what generative AI encompasses and its diverse applications, but also to provide insights into managing potential risks from both commercial and legal standpoints. Additionally, we aim to offer practical approaches to navigate these challenges whilst also staying up to date with the rapidly evolving landscape of AI generally, and with generative AI specifically. But, in order to understand generative AI, one must first establish a foundational understanding of AI in a broader context.

What is AI?

In the European Commission's proposal for a new Artificial Intelligence Act (AI Act) (as amended by the European Parliament on 14 June 2023), the term "AI systems" is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions,

recommendations, or decisions, that influence physical or virtual environments".

An immediate reflection to make is that the above EU legal definition of AI might seem broader than what is commonly associated with the term AI. For instance, the legal definition likely includes numerous current IT solutions in the market, going beyond advanced technologies and robots to also encompass systems used in everyday business and daily life.

Generative AI

What is generative AI?

Generative AI constitutes a subset of AI which involves creating models capable of producing new data, including text, images, or sound. These models mirror patterns and structures present in their training data, learning from existing datasets and subsequently employing this knowledge to create original content. A common example of generative AI is GPT (Generative Pre-trained Transformer), a series of AI models that includes GPT-3, developed by OpenAI. These models possess the capability to generate cohesive text based on the content they have been exposed to during training.

Challenges with generative AI

With a foundational understanding of Generative AI in place, we can now explore the specific issues and challenges that may arise in its various use cases.

Potential intellectual property issues

A highly debated issue revolves around the commercial utilization of AI-generated content produced through the training of AI on potentially copyrighted material obtained from web scraping. This practice has faced criticism, particularly when the AI tools are trained on copyrighted internet content without proper authorization. At the same time, the training of AI tools on a diverse range of works is vital to generate results effectively. Consequently, this practice has prompted numerous legal disputes, involving entities engaged in data collection as well as in the sale of AI-generated content. One discussion within this context is whether it conforms to existing copyright laws to use legally acquired images in databases, which are not subject to scraping prohibitions, for the AI training.

Another aspect related to generative AI and copyright, pertains to ownership of the outcomes produced by AI models. Whilst this matter remains far from resolved, the prevailing consensus today suggests that neither the AI model, the creator/user, nor the company that possesses the AI model can claim copyright over, for instance, an image generated by the AI, e.g., according to Swedish law, such a copyright claim would not be possible as no independent creative decisions are involved (as user rights are dictated by the terms and conditions established by the company that owns the AI model), and as a copyright creator must be a physical person.

Improper training of AI and additional commercial and legal implications

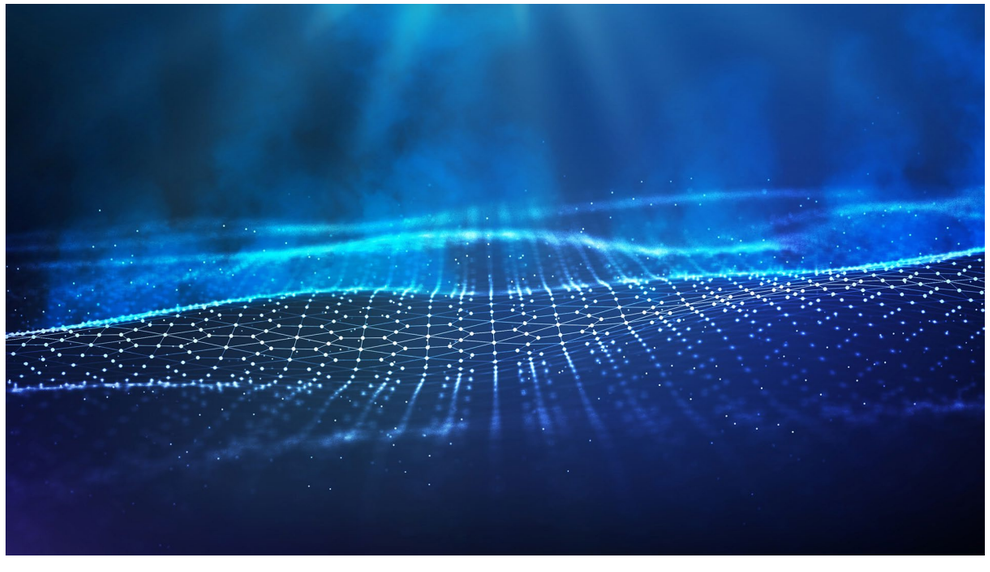
Another highly debated issue revolves around the challenge of preventing the intentional and improper training of generative AI. At the time of writing this article, there are few, if any, safeguards in place to prevent a group, nation, or company from intentionally training an AI system in a deceptive manner to further their own objectives. This scenario highlights the need to explore potential countermeasures. In theory, prospective solutions might encompass a variety of measures, such as:

I. Automatically "ranking" the reliability of the sources of information in an AI model;

II. restricting the AI model to gathering data solely from certain "authorized" sources and individuals; and

III. manually reviewing all information before allowing the AI model to utilize it as training data.

However, these suggested solutions are not without limitations. For instance, one might raise concerns about the feasibility of implementing solutions (i) from a privacy/GDPR perspective (as a substantial volume of data may be necessary to effectively and realistically evaluate the trustworthiness of the AI's information sources and as such information might include personal data which would in turn make the GDPR applicable), solution (ii) as it could, in some respects, seem counterintuitive and contradictory to the overarching objective of AI systems, which is to collect and process a vast amount of information, and as restricting an AI model to limited factual data, even if of high quality, would thus most likely have competitive drawbacks compared to a model trained in a more open manner, and (iii) as it may not be practically feasible, as actors might not be inclined to allocate the necessary resources, nor see the value in manually reviewing all information before the AI utilizes it as training data.



AI legislation

Although AI is currently largely unregulated, there are regulatory initiatives in progress. Foremost amongst these initiatives is the European Commission's proposition for a new Artificial Intelligence Act (the "**AI Act**").

The AI Act

The AI Act's objective is, e.g., to address potential AI related risks and establish a stronger framework for the use of AI in the EU. The regulation will apply to the provision of AI systems to the EU, regardless of whether the system providers are established within the EU or in a third country (i.e., any country outside of the EU or the EEA). It will also cover the use of AI system output in the EU even if the providers and users of the AI systems are located in a third country. In this sense, the AI Act bears a resemblance to the far-reaching scope of the GDPR.

The expansive reach of the AI Act is designed to prevent potential circumvention of the regulation, such as scenarios where personal data is collected within the EU, processed by a high-risk AI system in a third country, and then imported back for use in the EU as resulting output, all without the AI system being implemented within the EU market.

The regulation will apply not only to standalone AI systems, but also to AI systems integrated into other software products. Much of the software that is generally used on the market today may thus be covered by the AI Act to some extent.

Thus, if approved as suggested, the AI Act can be expected to have a large impact on the market for the provision of both advanced and everyday IT solutions and software.

Different Rules Depending on Risk

The AI Act adopts a risk-based approach, emphasizing various categories of AI system uses or practices over specific techniques for AI system operation. This approach can be likened to a four-tiered pyramid. Within this pyramid, the uppermost fourth tier categorizes and prohibits several AI practices considered unacceptable. These practices include the exploitation of vulnerabilities amongst specific individuals, which might be based on factors like age or physical and mental capabilities.

The third tier encompasses specific practices associated with high-risk AI applications. Whilst not explicitly banned, these practices are recognized as high risk and subject to particular requirements. Examples of AI systems falling into this high risk category include those used as safety components within critical infrastructure, such as road traffic, water and electricity supply, as well as AI systems used in the administration of justice and democratic processes.

When assessing a generative AI tool's compliance with the AI Act, a company should thoroughly evaluate all risk levels. However, for generative AI, the second tier, which underscores transparency requirements, is typically the most relevant. At this level, AI systems must, for instance, disclose that the content was AI-generated. Further transparency requirements, particularly applicable to generative AI, involve designing the model to proactively avoid producing illegal content and sharing concise summaries of copyrighted data used for training.

Additionally, the AI Act will enable EU member states to implement voluntary codes of conduct for AI systems not falling within the aforementioned risk pyramid.

Like the GDPR, the AI Act outlines substantial penalties for violations, with administrative fines ranging from 10 million to 30 million euros or 2-6% of the entity's total global annual revenue, whichever is higher.

Conclusions and takeaways

The development of AI is fast-paced, dynamic, and for some, either thrilling or daunting. Similar to many technological advancements, expecting the law to promptly and effectively adapt to AI's progress is likely an unrealistic prospect. Despite regulatory efforts and lawmakers' aims to maintain technology-neutral legislation, AI's development is likely to outpace legal adaptation. Consequently, it is inevitable that legally unregulated gaps will emerge, as well as that uncertainties surrounding the application of existing laws will persist. In summary, these circumstances lead to significant challenges and risks, such as those described above.

However, there are some practical measures that can be incorporated into daily routines in order to mitigate risk. To preserve confidentiality and protect sensitive data, it is essential to avoid feeding such information into AI systems. Additionally, it is important to recognize that AI-generated outputs may contain errors and thus require additional verification and scrutiny. Actors looking to implement or use an AI tool should ensure that routines are established, both before and after implementation. Understanding both the AI system and applicable regulations is further crucial for effective system training

and compliance. In contemplating the use of an AI tool, these considerations should guide the decision-making process. Finally, experience has taught us the significance of developing a thorough understanding of the technology itself, as well as the acute need to stay updated on regulatory developments. The AI Act may enter into force as soon as in 2024, and can be expected to extend beyond advanced technologies, to encompass systems used in everyday business and daily life. This means that covering all developments in this sector will be vital to stay competitive.

Sophia Spala
PARTNER
STOCKHOLM

Frej Thorgren
ASSOCIATE
STOCKHOLM

STOCKHOLM

Sturegatan 10
Box 1050
101 39 Stockholm

stockholm@setterwalls.se

GOTHENBURG

Sankt Eriksgatan 5
Box 112 36
404 25 Gothenburg

gothenburg@setterwalls.se

MALMO

Stortorget 23
Box 4501
203 20 Malmoe

malmoe@setterwalls.se