SETTERWALLS

FinTech Report 2022

SETTERWALLS

Introduction

Yet a strange year has passed since the last FinTech Report (2021) and I believe most people will remember this year as the year Russia invaded Ukraine (and the western world's response [sanctions] to Russia's military aggressions).

However, it is also a year which started out with an overwhelming optimism in the market, including a feeling of "the sky is the limit" in the sector, which suddenly turned into a possible recession around the corner. We expect investors to be pickier in the near future and it is likely that smaller and fewer checks will be written. Looking back, recent developments can only be defined by one word: unexpected. Thus, we have, over the last period, seen a declining desire to invest and the window for IPOs seems to be closed. On the other hand, we still see an ongoing strength in the payments sector and cross border payment projects, including talks about e-wallets and e-identification, as well as a growing appetite from foreign jurisdictions to make fintech investments in smaller deals, and VC rounds. As a reflection of the events in the past year, we see a significant increase in the focus of cyber security as well as national security interests.

This report aims to be a source for insights and inspiration into Swedish Fintech ecosystem for all categories, i.e. lawyers, investors, entrepreneurs/start-ups, established corporates /banks etc. In light of this, our FinTech Report 2022 has focused on subjects that we believe are "hot" and interesting, reflecting on the unpredictable era we currently are in.

Without any further delay, it is our pleasure to present the new issue of Setterwalls' FinTech Report. We hope that you will enjoy it.

- **The upcoming EU Crypto Asset Regulation (MiCA)– are NFTs *to be regulated like crypto*?**
- **Payment Service Providers – Are you (really) ready for the new proposed SCA requirements?**
- **The European Digital Wallet - an opportunity for FinTechs and established institutions alike**
- **Softening the blow? Potential limitations of applying GDPR fines under Swedish constitutional and administrative procedure law**
- **Amazon going biometric - pay with the palm of your hand**
- **Is the insurance and reinsurance sector up to date on the EIOPA Guidelines on outsourcing?**
- **Focus on protective security compliance increases – what to expect from the SFSA?**

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

The upcoming EU Crypto Asset Regulation (MiCA)– are NFTs *to be regulated like crypto*?

Initial proposals by EU institutions seemed to make it clear that NFTs were to be excluded from the upcoming MiCA Regulation. However, recent statements by an EU official indicate that the exemption may not provide much relief for NFT stakeholders since they may need to pass through the eye of a needle to not be covered by the proposed regulation's wide-reaching requirements.

Background

In the 2021 issue of Setterwalls' FinTech Report we focused on the European Commission's new legislative proposal on crypto-assets, *the Markets in Crypto-Assets Regulation* ("MiCA")[1], which was adopted on 24 September 2020.[2] As mentioned in the report, the Commission's intent is to provide for a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection. Furthermore, being the first regulatory framework at EU level for crypto-assets, the purpose is to bring further financial stability and clarity within the EU, while still allowing innovation and fostering the attractiveness of the crypto-asset sector.

The latest update on the legislative process is that the Council presidency and the European Parliament on June 30th, 2022, reached a provisional agreement on the MiCA proposal, announced on a press release by the Council.[3] Although the official text of the MiCA will have to wait until the formal approval process is completed, the press release revealed, albeit general, some of the terms of the agreement. These have been extensively discussed among crypto enthusiasts since the declaration.

One of the terms that was revealed is the exclusion of *non-fungible tokens* ("NFTs") from the scope of the MiCA. In contrast to regular cryptocurrencies, NFTs do not merely represent a business in the crypto-asset market, but also a type of art and legitimate ownership. However, recent announcements and analyses indicates that the assurance of the exclusion of NFTs may not tell the whole truth.

NFTs and MiCA – a mixed message

In the official press release it was stated that "Non-fungible tokens (NFTs), i. e. digital assets representing real objects like art, music and videos, will be excluded from the scope of the upcoming regulation, except if they fall under existing crypto-asset categories.".[4] However, despite this unambiguous statement in the press release, statements by an EU official and adviser for technological innovation at the European Commission, Peter Kerstens, has brought doubt to the extent of the exclusion. At the Korea Blockchain Week in August, Mr Kerstens remarked that the EU regulators have "a very narrow view of what is an NFT". This comment has led to numerous speculations among stakeholders on the crypto market regarding the potential regulation of NFTs. Hence, in lack of the official and final text of the MiCA, there is a great uncertainty whether and to what extent NFTs will be covered by the new rules on crypto and whether the carve-out of NFTs, as declared in the press release, only might provide a scant relief for NFT stakeholders from MiCA's onerous rules[5].[6]

NFTs today and tomorrow

The Market

NFTs have turned extremely popular in the crypto universe over the last years. NFTs are blockchain-based unique digital assets that are versatile, and where transactions are recorded and transparent. These qualities have led to numerous possibilities for the use of NFTs. For instance, an NFT linked to a digital artwork can ensure the buyer that the purchase relates to an authorised copy of the artwork, or a company could sell an NFT and link it to a virtual representation of a physical object. The NFT will, somewhat simplified, act like a digital certificate of authenticity for said objects. This contrasts with many existing crypto-assets, including cryptocurrencies like Bitcoin, which are fungible or interchangeable. Although NFTs have been around since 2014, they are becoming an increasingly popular way to purchase and sell digital artwork. For example, since November 2017 the staggering amount of $174 million has been spent on NFTs.[7]

[1] Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937
[2] Setterwalls' FinTech Report 2021, The new EU Crypto-asset legislation ("MiCA") – are the Wild West days of Crypto about to end? p. 12-17
[3] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
[4] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
[5] https://www.crypto-news-flash.com/nfts-will-have-similar-regulatory-rules-like-crypto-under-eus-mica-law/
[6] https://www.coindesk.com/policy/2022/08/10/nft-collections-will-be-regulated-like-cryptocurrencies-under-eus-mica-law-official-says/
[7] https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-an-nft-how-do-nfts-work/

Current regulatory environment
NFTs are currently not explicitly regulated in the EU. A national financial supervisory authority would have to make an assessment in each individual case on how to categorize an NFT, based on the specific features of the relevant NFT, and then assess whether the NFT falls under any current financial market regime (rules to consider would for instance be e-money and payment services regimes, MiFID II[8] and prospectuses rules).

NFT collections – especially in limbo?
Although the press release stated that NFTs will be excluded from the scope of the MiCA Regulation if they do not fall under existing crypto-asset categories, Mr Kerstens' abovementioned remarks implies that only a few NFT-assets will in practice benefit from such exemption. Mr Kerstens explained his statement by adding that "If a token is issued as a collection or as a series – even though the issuer may call it an NFT and even though each individual token in that series may be unique – it's not considered to be an NFT, so the requirements will apply."[9]

The Council's press release statement refers to "digital assets that represent real objects such as art, music and video". Depending on the final definition of NFTs in the MiCA, NFTs which do not qualify as such could then be subject to the new regulation. According to Kersten, NFTs that have originated out of a collection, where each one of the NFTs are unique, may not be considered as an exempt NFT under the definition in MiCA and the provisions therein will apply. An example of such NFT collections are NFTs issued in multiple copies and representing rights to different types of performances,[10] such as the Bored Ape Yacht Club which is one of the most popular and valuable NFT collections in the world. This specific collection is made up of 10,000 unique non-fungible tokens on the Ethereum blockchain depicting ape avatars with various characteristics.[11]

This reveals the challenges (due to the versatile and complex structure of NFTs) as well as points to the importance, to define the concept of NFT as precise as possible. Hence, the breadth of the definition of an NFT in the MiCA will play an important role when determining the scope of the MiCA in relation to NFTs.

What if MiCA will apply to NFTs?
As mentioned above, if an NFT has the characteristics and therefor may be categorised as one of the existing crypto-assets defined in and covered by MiCA, e.g., a collection or series of NFTs, it may be subject to the MiCA and the issuer would have to comply with the requirements set out therein. This would mean that issuers of NFT collections might be considered as crypto-asset issuers and would have to publish a white paper setting out details of the protocol used by the NFTs and would be forbidden to make outlandish promises about future value that could mislead people into buying their products.

Since a white paper is a lengthy regulatory document broadly equivalent to the prospectus drafted for securities, it may be questioned if it is feasible for an NFT issuer to publish a white paper for the creation of every singular NFT. Furthermore, this may also mean that NFT-specialized marketplaces would have to seek regulatory authorization to be crypto assets service providers, which some mean could possibly stifle the innovation in the NFT industry[12].

Final remarks
To sum up
Whether a specific NFT will be subject to MiCA or not depends on whether the NFT may be covered by one of the already proposed crypto-asset categories. However, for NFTs which cannot be "re-classified" in such way, one will have to resort to the regulations already in force and applicable to solve possible legal loopholes. Thus, the decisive factor on which regulation that will apply to NFTs will in such cases be determined by the character of the NFT as such, although most NFTs will fall outside of the scope of current financial regulations.

The main reason for NFTs, at least as a starting point, being excluded from the scope of MiCA is probably due to the very nature of NFTs which differs from a

[8] 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
[9] https://www.coindesk.com/policy/2022/08/10/nft-collections-will-be-regulated-like-cryptocurrencies-under-eus-mica-law-official-says/

[10] https://en.cryptonomist.ch/2022/07/15/micaprovisional-agreement-reached/
[11] https://www.nftgators.com/nft-collections/
[12] https://www.coindesk.com/policy/2022/08/10/nft-collections-will-be-regulated-like-cryptocurrencies-under-eus-mica-law-official-says/

"traditional" crypto currency like Bitcoin. NFTs are first and foremost a type of art and manifestation of legitimate ownership which have however turned into a major business itself. Yet, some claim that NFTs have become more similar to cryptocurrency. This since the NFT market has been as vulnerable to securities-style rate changes, money laundering, and other illicit purposes such as wash trading, as any other crypto-asset markets[13].[14]

Considering the purposes of the MiCA Regulation, to preserve financial stability while allowing innovation and fostering the attractiveness of the crypto-asset sector, it may be questioned why NFTs should not be covered by MiCA instead of the semi-solution which the proposal seem to be offering at the moment.

The next step of the legislative process
The provisional agreement accounted for above is subject to the approval of the Council and the European Parliament before going through the formal adoption procedure. As also stated in the press release from the Council, the European Commission will be tasked to, within 18 months, prepare a comprehensive assessment and, if deemed necessary, a specific, proportionate, and horizontal legislative proposal to create a specific regime for NFTs and address the emerging risks of such new market.[15]

It will indeed be interesting to learn what emerges from the final draft of the MiCA as well as the potential legislative proposal from the Commission on NFTs, in particular how NFTs will be defined. For the time being, MiCA's applicability on NFTs will most likely remain a hot topic which will leave issuers of, and service providers in relation to, NFTs with significant uncertainty while imposing more pressure on the EU institutions on how NFTs should be regulated in the future.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Fredrik Svensson
ASSOCIATE
STOCKHOLM

[13] https://www.moonstats.com/news/nfts-to-be-regulated-like-crypto-under-mica-law-eu-official/
[14] https://www.coindesk.com/learn/what-is-nft-wash-trading/
[15] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

Payment Service Providers – Are you (really) ready for the new proposed SCA requirements?

According to a recent Government proposal, you as a payment service provider must apply strong customer authentication ("SCA") when a payer uses a payment method that involves payment deferral, e.g. selects invoice payment as a payment method when purchasing goods or services online. Otherwise, you may be in violation of the proposed requirements, which may result in an intervention from the Swedish FSA (Swedish FSA interventions include a warning, penalty fee and/or revocation of permits).

Today, the Payment Services Act (2010:751) requires payment service providers to apply SCA when a payer logs into its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel that may pose a risk of fraudulent activities or other forms of abuse. However, through the Government's proposal it is clarified that the requirement on SCA extends to situations which, according to the general opinion, has previously not been considered being a payment service.

Who is concerned by the proposed SCA requirements?
A payment service provider – e.g. a bank or a payment institution – under the Payment Services Act will have to apply SCA when a payer uses a payment method that involves payment deferral, e.g. selects invoice payment, if the payment method comprises of the payment service provider issuing an invoice to the payer and transferring funds to the payee (and the payment service provider thus is facing the credit risk).

As of now, the proposal does not appear to cover the relatively common arrangement when payment deferral is granted by the e-retailer himself and the claim for payment is then transferred to be collected by a payment service provider within a factoring arrangement. Such an arrangement falls outside the scope of the proposal and thus means that no SCA requirements apply in the case of payment methods where payment deferral is granted by the e-retailer himself.

What does the SCA requirements oblige you to do?
Today some payment service providers only require the consumer to provide certain personal data (such as name, postal address and social security number) in order to use invoice as a payment method when purchasing goods or services online. Such an offering will not be enough to fulfil the SCA requirements.

SCA refers to an authentication that is based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) which are independent of each other, so that the breach of one does not compromise the reliability of the others, and is designed to protect the credentials from unauthorized access. Such an authentication method is often called multi-factor authentication and examples of identification methods that meet these requirements are the use of e-ID or a bank card reader.

Next steps
The Government has referred the proposal to the Council on Legislation, which had no objection to the proposal. The next step is for the Government to process the proposal further and then submit it as a bill to the parliament for approval.

In its referral to the Council on Legislation, the Government proposed that the changes to the Payment Services Act shall enter into force on 1 January 2023.

To conclude
It is recommended that you in the near future review your existing offering and arrangement to ensure compliance with the proposed SCA requirements. It is also important to keep up to date with the legislative process, in order to be ready if and when the changes to the Payment Services Act enter into force.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Hanna Salajin
ASSOCIATE
STOCKHOLM

The European Digital Wallet - an opportunity for FinTechs and established institutions alike

Actors in the fintech market are pushing the technical development and the financial markets to adapt to customer needs. This also affect legislators which need to adapt legal frameworks to ever-changing market conditions. In turn, fintechs and established financial institutions must stay up to date with the current legislation which affect the digital financial infrastructure. A current push of interests is the European Commission's focus on enabling use of digital identities for better access to financial services.

The European Commission (the "Commission") has proposed to amend the eIDAS-Regulation[1] on electronic identifications and trust services to boost more cross border authentications and identifications (the "Proposal").[2] The Proposal introduces a European Digital Identity Wallet ("Digital Wallet") to facilitate a new European Digital Identity Framework. In this article we will look closer at some of the Commission's proposed changes to the eIDAS-Regulation, and how they could benefit fintechs and established financial institutions (jointly referred to in this article as "Financial Businesses").

Background

The eIDAS-Regulation has laid a foundation for an identification and trust services market and better cross-border authentication and identification (jointly referred to in this article as "identification") in the EU. This by establishing a network for notified national electronic identification ("eID") schemes. Persons that have obtained an eID are able to digitally prove and verify their identities via mobile phone or computer when accessing digital services.

The main types of trust services under the eIDAS-Regulation are electronic signatures, electronic seals and electronic time stamps. Trust services are in turn categorized into different qualifications levels depending on their attributes.

The eIDAS-Regulation has brought many benefits to Financial Businesses already by providing the conveniences of easier identification of customers, which in turn helps to facilitate regulatory compliance and better customer access. However, the frequency of cross-border identifications is surprisingly low, in parts because only (by approximation) 60 percent of EU's citizens have access to eIDs that function for cross border identifications. Another factor is that very few public digital services accept cross border identifications for access.[3] To meet new market demands and policy objectives, the Commission has concluded that the eIDAS-Regulation needs to be amended to boost more cross border identifications by focusing on effectiveness, efficiency, and coherence.

The Proposal

The Commission is proposing the following additions of interest to the eIDAS-Regulation under a new, so called, European Digital Identity framework:

i. Member States must provide citizens and businesses with a Digital Wallet capable of linking their national eID with proof of other personal attributes. The Digital Wallets could be issued either by a Member State, under a mandate from a Member State, or independently but recognised by a Member State.

ii. The Digital Wallet must be accepted by public and (some) private services in all Member States. Such private services are services that by law or contract are required to use strong user authentication for online identification which includes services in areas such as banking and other financial services.[4]

The Digital Wallet is a technical solution that goes beyond the functions of the eIDAS-Regulation compliant eIDs but is not separate from that system. The Digital Wallet will allow EU citizens to identify themselves via eIDs, but also store and make available identity data, credentials, and other personal attributes and to make qualified electronic signatures or stamps,[5] most likely through a smart phone or computers.[6]

The Digital Wallet could provide for easier strong user authentication which benefits both Financial Businesses and customers in cases when strong user authentication

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[2] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.
[3] The Commission's evaluation of the eIDAS regulation, COM(2021) 290 final, p. 4.
[4] Section 28 and article 12b in the Commission's explanatory memorandum on amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.
[5] Article 3.42 in the Commission's explanatory memorandum, COM/2021/281 final.
[6] Agency for Digital Government's report on a digital wallet, DIGGs ärendenummer 2022-33.

is necessary for the provision of financial services, e.g. financial services provided by banks. It will also be easier for users to store and make available some basic personal data such as university diplomas, drivers licenses or bank cards instead of having to carry such documents in physical form.[7]

General requirements for Financial Businesses

In general, Financial Businesses have certain hurdles to overcome to reach or establish themselves on a specific market. In most cases, a new service must be able to adapt to an already established market and infrastructure, which requires interoperability and mutual recognition between systems and functions. For an example, think of the interoperability of systems that is required to perform a payment from one bank account to an account in another bank. Secondly, customers must be receptive to the offered service, in particular when the service requires certain technical understandings and computer literacy among the customer base. In this regard, different markets are susceptible to new digital services to a different degree, depending on their digital maturity. Thirdly, regardless of the above, the Financial Businesses must comply with regulatory requirements. In the next chapter we will look at the current situation in Sweden for Financial businesses and use of eIDs.

The situation in Sweden

Any amendment to the eIDAS-Regulation will have varying effects on the different Member States. Digitally mature countries such as Sweden have already verified eIDs.[8] Subsequently, Swedish Financial Businesses rely on Swedish eID to either

[7] Agency for Digital Government's report on a digital wallet, DIGGs ärendenummer 2022-33.
[8] Section 3.1 in the Agency for Digital Government's report on a digital wallet, DIGGs ärendenummer 2022-33; and https://www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering.

identify users or to identify representatives of the business. Having access to a Swedish eID means that Financial Businesses potentially have:

i. better access to customers since the customers will be able to identify themselves through e.g., their smart phones,

ii. better access to necessary information and digital services from banks and public authorities since a general requirement for using such services is the ability to identify the user or the representative of the business.

iii. streamlined regulatory compliance since it becomes easier to uphold KYC-requirements under the applicable AML/CFT legal framework and strong customer authentication requirements under payment services-legislation since customers can identify themselves through trusted services.

The current Swedish eID system rely fundamentally on the Swedish population register, meaning that a person applying for eID generally must have a Swedish personal identity number or a so-called coordination number. With certain exceptions, this means that persons who do not have a Swedish personal identity number or a coordination number often cannot obtain a Swedish eID under the current system. Many digital services in Sweden, which are provided by public authorities and Financial Businesses, are mainly accessible based on user identification via Swedish eIDs. As a result, foreign fintechs and customers that cannot obtain a Swedish eID can be excluded from these services and the benefits of Swedish eID.

What could the proposal entail for Financial Businesses?
As already established, Financial Businesses have certain hurdles to overcome to reach or establish themselves on a specific market. Below we will look at specific things that the Proposal potentially could improve for Financial Businesses.

Wider customer base
The introduction of a mandatory requirement for each Member State to issue a Digital Wallet and the requirement that other Member States accept these Digital wallets could affect the size of the customer base for Financial Businesses since, i) more people will have a access to a functioning eID and measures to store and make available some basic personal data, ii) more Member States and persons may grow accustomed to eIDs and electronic signatures instead of manual identifications and signatures, leading to more persons being susceptible to use digital financial services and iii) cross border identifications could become easier which allows for better cross border access to digital services within the EU.

Strong customer authorisation and know you customer requirements on a cross border basis
There is a general requirement under PSD2 that payment service providers shall perform strong customer authorisation when providing payment services. According to the Swedish Agency for Digital Government ("DIGG"), strong customer authorisation under PSD2 corresponds to approximately the second highest trust level for eIDs under the eIDAS-Regulation.[9] Similarly, the current AML/CFT-rules includes KYC requirements for the provision of certain services and already allows for the use of eIDs to identify customers.

In Sweden, many banks and payment service providers rely on Swedish eIDs which are registered as the second highest trust level under the eIDAS-Regulation to uphold these requirements. We believe that the Proposal can entail that Financial Businesses can gain better access to new markets by virtue of upholding better compliance with payment service-legislation requirements and AML/CFT-requirements in different jurisdictions.

Greater access to public information and other digital services
Financial Businesses must be able to digitally identify themselves with other service providers to, e.g., open a company bank account or to perform necessary daily operations such as signing of digital documents. In Sweden, foreign Financial Businesses often struggle to access necessary services. Hopefully, the Commission's Proposal will provide easier access to necessary digital services for such Financial Businesses so that these can compete on a more levelled playing field.

To conclude
A cohesive and easy to use Digital Wallet, with the inclusion of different eIDs, electronic stamps and certificates, can be to the benefit of Financial Businesses that must both uphold regulatory requirements to identify customers and convey trust in the offered solutions to the customer base. The Proposal can perhaps also bring other benefits to Financial Businesses such as boosted efficiency for operations that require approvals, identification, exchange of important document, or allow for greater access to public information and necessary digital services.

There is still a lot of work to be done before the results envisaged above can become realities, with legislative and technical efforts taken in the parallel. Yet, based on statements from a representative of the Commission, there may be a fully operational system for Digital Wallets as early as by 2024.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Carl Broberg
ASSOCIATE
STOCKHOLM

Softening the blow? Potential limitations of applying GDPR fines under Swedish constitutional and administrative procedure law

The size of potential administrative fines for non-compliance is a significant driver for companies' efforts to become compliant with the extensive requirements under the GDPR. These administrative fines also entail a significant risk for any business that involves processing of personal data.

However, recent legal developments have put the application of such fines in potential conflict with Swedish administrative procedure and constitutional law – which potentially could limit the scope and possibility for the Swedish Authority for Privacy Protection (the "IMY") to apply administrative fines in some cases. In this article, we look into two separate reviews and decisions by the IMY where the potential conflict with the Swedish administrative procedure and constitutional law has come into play and what this could mean for other cases where companies are supervised or reviewed by the data protection authority in Sweden.

First case: IMY recently issued a decision against Verifiera AB[1] ("**Verifiera**") in relation Verifiera's database, which is a search service for court decisions that provides sensitive personal data in a register. The database has a certificate of publication (Sw. *utgivningsbevis*), which means that it falls under the Fundamental Law on Freedom of Expression (Sw. *yttrandefrihetsgrundlagen*). For this reason,

[1] IMY's decision against Verifiera AB (IMY-2022-1621).

the database is also exempt from certain obligations under the GDPR[2], under the exception for journalistic purposes[3]. This is the main issue that was examined in the IMY decision. In short, IMY concluded in its decision that Verifiera's processing of personal data violates the GDPR, and that the exception for journalistic purposes therefore does not apply. This exception has not previously been applied by the IMY or any court, which has resulted in different interpretations of the exemption by practitioners.

To summarize, the decision from IMY contains one main question, whether the GDPR applies on certain companies conducting journalistic business, including companies with a certificate of publication, or if constitutional law takes precedence over the GDPR. This is a fundamentally interesting conflict and balancing act between the Swedish constitution and the GDPR, which will have a decisive significance on the application of the GDPR for companies that conduct journalistic business, or act under a certificate of publication. IMY's decision has been appealed by Verifiera to the administrative court and we will monitor this closely.

Second case: In December 2020, IMY announced several decisions[4] against eight health care providers and regions that were considered to be in violation of the GDPR[5], among other things, regarding their authorization assignment for medical record systems. The authority concluded that seven of the health care providers did not limit the users' access authorization to the respective patient journal system to what is strictly necessary for the performance of their tasks. Therefore, the health care providers had not taken appropriate measures to ensure and be able to demonstrate a sufficient level of security for the personal data in the medical record systems, which IMY found to be in breach of the GDPR. The deficiencies and the non-compliance with the GDPR were so serious, according to IMY, that they result in administrative fines of between 2,5 to 30 million SEK.

Five of the decisions were appealed to the Administrative Court of Appeal in Stockholm, which subsequently (and, according to some commentators, surprisingly) overturned the Administrative Court's ruling and IMY's decision on administrative fines, as well as the authority's injunction to remedy the deficiencies regarding the disclosure of competence to the medical record systems.[6]

In its ruling, the Administrative Court of Appeal held that the burden of evidence rests with the supervisory authority in relation to administrative fines, and that such fines under the GDR must be seen as corresponding to a criminal penalty. The

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection).
[3] See Article 85 of the GDPR.
[4] IMY's decision against Sahlgrenska Universitetssjukhuset (DI-2019-3840), Region Västerbotten (DI-2019-3841), Region Östergötland (DI-2019-3843), Capio S:t Görans Sjukhus AB (DI-2019-3846), Karolinska Universitetssjukhuset (DI-2019-3839), Digital Medical Supply Sweden AB (KRY) (DI-2019-3845), Aleris Sjukvård AB (DI-2019-3844) and Aleris Närsjukvård AB (DI-2019-3842).
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[6] Case numbers 4471-21, 4511-21, 4540-21, 4548-21 and 4611-21.

supervisory authority's burden of evidence should therefore, for reasons of legal security, be set high – the court compared it to the burden of evidence required to impose a tax penalty under Swedish tax law, concluding that that the same high burden of evidence also shall apply for fines under the GDPR. The requirement in Swedish cases regarding imposing of fines under the GDPR is therefore that the evidence must clearly provide substantial support that the conditions for deciding on an administrative fine are met. In practice, this means that IMY cannot place the burden of evidence on the specific company according to the documentation obligation for data controllers under the GDPR[7]. The authority has a high burden of evidence in relation to the imposition of fines and must therefore provide substantial and in detail evidence on the non-compliance of the GDPR, which opens to counter arguments and defense by the company. In the ruling, the court thus found that IMY failed to live up to this evidentiary requirement, indicating that IMY has not applied the GDPR in light of Swedish administrative procedure law, e.g. with regard to the evidentiary requirement for the authority's evidence in supervisory cases.

In our opinion, this ruling entail that the imposition of administrative fines under the GDPR might be narrower under Swedish administrative procedure law, for evidentiary reasons, providing a potentially higher threshold than indicated in the GDPR. This could potentially limit the scope and possibility for IMY to apply administrative fines in some cases and may provide for lower fines in some other cases. It may also

[7] See e.g. article 5.2 of the GDPR.

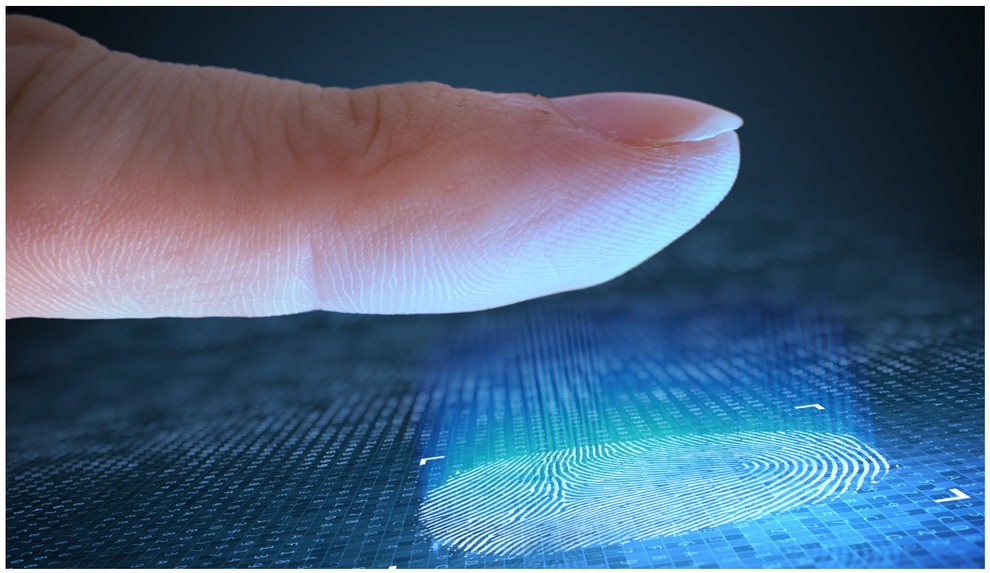
provide for an additional defensive argument in any Swedish proceedings regarding administrative fines. Whether this is unique for the Swedish application of GDPR fines remains to be seen.

As mentioned in this article, the two decisions from IMY, and the rulings from the Administrative Court of Appeal indicate that there is a conflict between the GDPR and Swedish administrative procedure and constitutional law, which potentially may narrow the scope and the application of the GDPR, in relation to the imposition of administrative fines by IMY.

However, the significance of the Swedish administrative procedure and constitutional law in relation to application of the requirements and sanctions of the GDPR are still far from settled and further developments are to be expected. Upcoming rulings will likely further expand on whether Swedish specific conditions shall apply, in relation to the requirements and sanctions of the GDPR.

Niklas Follin
PARTNER
STOCKHOLM

Alexandra von Perner
ASSOCIATE
STOCKHOLM



Amazon going biometric - pay with the palm of your hand

New technologies based on biometric data makes payments easier and faster. Amazon is one of the actors on the market that has invested in the development of a biometric system enabling in-store purchases by using the hand palm as a means of payment. Although such innovation may make the everyday life more effortless, there are some legal aspects to be considered.

In 2020, Amazon introduced its innovation called *Amazon One*. The biometric system *Amazon One*, which has become an alternative to traditional point of sale systems, allows customers to register the palm of their hand, payment card and phone number at the entry of a store, and then pay at the checkout point simply by the customers holding the registered hand palm over a scanning device. Beyond retail stores, *Amazon One* could also be used in as an example stadiums and office buildings, in order for people to perform more everyday activities effortless. Having tested the technology in Amazon's own stores in the US, *Amazon One* has been licensed to different third parties, and in August this year it was announced that the biometric system will now be licensed to an additional 65 Whole Foods stores across California.

There are also other actors that advocate payment by biometric solutions. In May this year, Mastercard launched a pilot project enabling payments in retail stores by facial recognition or fingerprints. The technology has already gone live in retail stores in Brazil and the aim is to roll it out globally this year. Furthermore, the Swedish financial company Rocker launched an innovation this year that represents

the first biometric payment card in Sweden. Instead of entering a PIN code, the card enables purchases through fingerprint ID, regardless of the amount of the purchase. The card is certified by Visa and can be used in card terminals worldwide. Worth to mention is that the Swedish company BankID, a company owned by several large Swedish banks and which provides an electronic identification system, soon will launch a biometric system enabling transactions via facial recognition.

Actors on the market consider biometric payment systems to not only bring practical and efficiency benefits, but to also be less risky than traditional systems in terms of integrity. Among other things, it is claimed that the technology increases security and prevents counterfeiting. However, despite the many benefits, biometric payment systems raise a host of privacy law concerns and there are also other legal aspects to be considered.

According to the Data Protection Regulation ("**GDPR**"), biometric data is considered as personal data of sensitive nature which requires stronger protection than other types of personal data. As an effect thereof, the processing of such data requires, when at all allowed, as a main rule specific and explicit voluntary consent by the person to whom the data belongs.

As a result of a proposed new EU legislation – a regulation on artificial intelligence ("**AI**") - additional requirements are in the pipeline and the provisions are planned to be fully applicable in the second half of 2024. Like the GDPR, the proposed AI regulation will apply, not only to actors within the EU, but also to foreign actors that bring and use AI systems in the EU.

Since the suggested rules are intrusive, providers of biometric payment systems should carefully consider them and analyse their solutions against them, to ensure that their services are satisfactory compliant and otherwise, if not, to ensure that necessary adaptions can be made to avoid investing in systems that may be prohibited by the new EU regulation.

In conclusion, new innovations bring new possibilities but the legal landscape sets frames for what may be provided, and since that landscape is under continuous change and development, it is necessary to stay updated.

Sophia Spala
PARTNER
STOCKHOLM

Rojda Aydin
ASSOCIATE
STOCKHOLM

Is the insurance and reinsurance sector up to date on the EIOPA Guidelines on outsourcing?

The EIOPA Guidelines on outsourcing agreements to cloud service providers, with a compliance deadline by the end of this year, imposes a heavy compliance burden on the insurance and reinsurance sector and the deadline for reviewing its cloud outsourcing agreements is quickly approaching. However, due to the lack of attention concerning the implementation of the sector specific guidelines there is a valid question to be raised: is the insurance sector up to date on the implementation of the EIOPA Guidelines?

Background

Recent cyber-attack demonstrates the vulnerability and risks that the insurance sector faces and shows the importance of secure IT systems containing sensitive personal data. In the end of October this year, Australia's largest health insurance company, Medibank, announced that it had been subject to a cyber-attack, where the hackers came across personal data of all four million customers. The hackers behind the attack demanded a ransomware to be paid and threatened to otherwise reveal medically sensitive data about known customers.[1]

The importance of outsourcing functions to cloud service providers has increased rapidly in many industries. Outsourcing data processing and storage capacity to

[1] https://computersweden.idg.se/2.2683/1.772062/medibank-hackat?utm_source=dmdelivery&utm_medium=email&utm_campaign=CS%20Senaste%20Nytt%20KV%C3%84LL%202022%202022-10-26%2015%3A50%3A34

cloud service providers reduces the cost of hosting, infrastructure and software and can help streamline IT expenditure leading to greater performance, flexibility, and adaptability.[2] However, as shown in the Medibank cyber case, regular security breaches emphases that cyber-attacks are a growing concern which undermine confidence and represents a fundamental threat to businesses in all sectors. Given the sensitive personal data which in many cases can be processed by the insurance sector and the potential exposure this entails, it is of great importance to make the financial sector cyber resilient.

The European Insurance and Occupational Pensions Authority's ("**EIOPA**") Guidelines on outsourcing agreements to cloud service providers ("**EIOPA Guidelines**"), which entered into force on 1 January 2021, serve to identify such risks and to ensure a secure cloud outsourcing infrastructure within the insurance sector. In addition, insurance undertakings must review and amend existing arrangements for cloud service outsourcing relating to critical or important operational functions or activities in accordance with the EIOPA Guidelines and notify the Swedish Financial Supervisory Authority of such agreements by 31 December 2022.

However, despite the closely emerging deadline to review, amend and notify existing arrangements for cloud service outsourcing agreements, the implementation process of the EIOPA Guidelines has been followed by comparatively less attention unlike when the similar Guidelines on outsourcing arrangements from the European Banking Authority entered into force on three years ago ("**EBA Guidelines**"). One can not but wonder how the implementation process has gone for the industry? Can this relative silence be explained by the insurance sector being more prepared for this type of regulation or is there still work to be done to implement the EIOPA Guidelines?

Why is there no buzz?
Although the EIOPA Guidelines imposes a stricter and heavier regulatory burden on the insurance sector compared to the prior sector specific requirements on internal governance, and even though a violation of the EIOPA Guidelines may be subject to administrative fines or revocation of license, the EIOPA Guidelines have received seemingly little attention compared to when the EBA Guidelines were introduced.

The EIOPA Guidelines apply to all cloud outsourcing arrangements by insurance undertakings, but there is a particular focus on the outsourcing of critical or important operational functions or activities to cloud service providers. Moreover, the EIOPA Guidelines impose the undertakings to maintain a record of its cloud outsourcing arrangements including information on, e.g., the contract and on the service provider[3]; conduct a risk assessment before entering into a cloud outsourcing[4]; conduct a due diligence on the cloud service provider[5]; and include certain clauses in an agreement with any cloud service provider when outsourcing critical or important functions.[6]

[2] The European Commission FinTech Action plan (COM(2018) 109 final), p 11.
[3] Guideline 5.
[4] Guideline 8.
[5] Guideline 9.
[6] Guideline 10.

Indeed, the EIOPA Guidelines imposes a great administrative weight on insurance undertakings and a need for a well-functioning internal governance. Considering this, as well as the quickly emerging deadlines, it is surprising that the EIOPA Guidelines have not been preceded by a more intense discussion regarding the implantation and its impact on the insurance sector.

Is the insurance sector ready for the EIOPA Guidelines – what does the indications tell us?

The predecessors of the EIOPA Guidelines

The insurance sector's potential silent treatment of the implementation might be understood in light of the regulations this sector already is obliged to comply with, which may have made it easier for the industry to adopt the new EIOPA Guidelines. The EIOPA Guidelines are based on the Solvency II Directive[7], the Delegated Regulation[8], and EIOPA's guidance on System of Governance.[9] Hence, the EIOPA Guidelines may be seen as an expansion of the legislative requirements contained in these regulatory frameworks.

[7] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
[8] Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

The abovementioned regulatory frameworks contain requirements similar to those in the EIOPA Guidelines. Furthermore, the EIOPA Guidelines aim to provide guidance on how the outsourcing provisions set forth in the Solvency II Directive should be applied in case of outsourcing to cloud service providers. In addition, the EIOPA Guidelines is meant to be understood considering the EIOPA Guidelines on System of Governance, in which similar compliance regulations in relation to outsourcing of critical or important operational functions and activities may be found, inter alia, written notification requirements and audit rights.

However, similar legal frameworks also existed for the banking sector when the EBA Guidelines were introduced, which thus does not explain why the EBA Guidelines were followed with greater attention.

Comparison to EBA Guidelines – is the insurance sector now better equipped?

Although the scope of the EIOPA Guidelines (mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers) is narrower than the EBA Guidelines, the insurance sector may have had an advantage if complying with the EBA Guidelines before the implementation of the EIOPA Guidelines.

EIOPA has explicitly stated that the EIOPA Guidelines have been, to some extent, kept aligned to the EBA Guidelines in order to have market consistency and to foster the harmonisation of the practice related to cloud outsourcing across sectors. The similarities in definitions, wordings, and requirements between these two guidelines may be explained by the fact that the risks associated to this practice are similar across sectors, as well as by EIOPA's purpose of avoiding potential risks of regulatory fragmentation.[10]

Furthermore, when the EBA Guideline were first introduced, the *Swedish Financial Supervisory Authority* urged other regulated sectors, including the insurance sector, which did not fall within the scope of the EBA Guidelines, to comply with the EBA Guidelines as well. This "false start" is likely to have given the insurance sector an advantage in complying with the requirements set out in the EIOPA Guidelines. This is also confirmed by a survey conducted by the Swedish Financial Supervisory Authority where especially the life insurance companies proclaimed that they already assessed that they complied with the majority of the requirements set out in the EIOPA Guidelines.[11]

The number of outsourcing agreements notified to the Swedish Financial Supervisory Authority – what does it tell us?

According to the Swedish Financial Supervisory Authority's records of matter registrations, the insurance undertakings are keeping up the pace with the requirements set out in the EIOPA Guidelines. When reviewing the number of outsourcing agreements notified by the largest insurance undertakings in Sweden to the Swedish Financial Supervisory Authority, the records display a clear trend that insurance undertakings are active in this process. Although the records of registration do not reveal whether these outsourcing agreements concerns cloud service providers, it shows a clear distinction of the number registered outsourcing agreements before and after the EIOPA Guidelines entered into force.

In addition, the records also entail that the insurance undertakings started to submit its outsourcing agreements early upon the introduction of the EIOPA Guidelines, indicating that the insurance undertakings were familiar with the procedures and that it had already implemented adequate internal routines. The fact that the insurance companies were quick to register their outsourcing agreements also suggests that the companies had already adopted the EBA Guidelines while awaiting the EIOPA Guidelines, as implied above.

Final remarks

The fact that the insurance sector, to some extent, already have been working with compliance in relation to the EBA Guidelines prior to the introduction of the EIOPA Guidelines, as well as the fact that most insurance companies have started notifying outsourcing agreements to the Swedish Financial Supervisory Authority, indicate that the insurance sector is well prepared for the EIOPA Guidelines. However, despite the seemingly proactive indications, there is still work to be done and some

[10] Final report on public consultation 19-270 on guidelines on outsourcing to cloud service providers.
[11] FI dnr 20-19345.

insurance companies likely have more work cut out for them than others, if to meet the deadlines and to be compliant with the EIOPA Guidelines when procuring new IT services henceforth.

As for now, it is due time for the insurance sector to get their outsourcing arrangements in place and to comply with the EIOPA Guidelines, and we will have to await the final verdict of whether the sector already has done its proactive implementation work, or if the deadlines will take the insurance undertakings off-the-cuff. It will indeed be interesting to see how many notifications that will be received by the Swedish Financial Supervisory Authority and whether the insurance sector's compliance with the EIOPA Guidelines will be supervised by the Swedish Financial Supervisory Authority as of 2023. And for the time thereafter, the work to ensure compliance with the EIOPA Guidelines, in both existing and new outsourcing arrangements, will continue.

Niklas Follin
PARTNER
STOCKHOLM

Fredrik Svensson
ASSOCIATE
STOCKHOLM

Focus on protective security compliance increases – what to expect from the SFSA?

With increasing threats to information-, physical- and personnel security, especially in times of escalating geopolitical instability, Sweden has strengthened its regulatory framework regarding protective security. The Protective Security Act (*Sw*. Säkerhetsskyddslagen (2018:585)), which came into force about three years ago, has seen its scope widened several times and has entailed an increased awareness amongst operators within the financial sector on the importance of security issues. In this article, we focus on the new supervisory structure within the area of protective security in the financial sector and provide our thoughts on what could be expected from the Swedish Financial Supervisory Authority (*Sw*. Finansinspektionen) (the "SFSA").

The reform of the supervisory structure

In the 2021 issue of Setterwalls' FinTech Report we focused on the Protective Security Act and a then recent Government Bill with proposed changes to it.[1] The proposals in the Bill were later adopted and came into force on December 1st 2021. As mentioned in our 2021 report, one of the important features of the Government Bill was that supervisory authorities were given investigative powers and the possibility to order operators to take certain measures subject to a conditional fine. The supervisory authorities were also given the power to decide on administrative sanctions against those that do not comply with the requirements of the protective security framework.

[1] Setterwalls' FinTech Report 2021, *ProTechtive Security (Sw. Säkerhetsskydd) – who does it concern?*

Aside from these features, another important proposal in the Government Bill that was also adopted and came into force on December 1st 2021 was the changes to the supervisory structure. The Government Bill mentioned that several shortcomings in the security inspection activities had been identified, some of which were related to the design of the supervisory structure. Examples of those shortcomings were that the supervision carried out was generally limited and some supervisory authorities did not carry out any supervision at all. It had also been found that some supervisors lacked the necessary factual and supervisory knowledge. On this basis, the Government considered that a reform of the supervisory structure was needed. There was also a need for a broad increase in ambition and knowledge in the area of protective security supervision.[2]

A new supervisory authority for the financial sector

Since the changes to the Protective Security Act came into force on December 1st 2021, the supervision has been carried out on a sectoral basis. For the financial sector, the SFSA is the supervisory authority and it thus supervise individual Swedish operators, as well as corresponding foreign operators established in Sweden, and actors with whom the operators have concluded security protection agreements.[3]

The SFSA has the power to issue regulations on protective security, which supplement the regulations of the Security Service (*Sw*. Säkerhetspolisen). Within its area of supervision, the SFSA also has a responsibility to provide guidance on protective security, decide on placement in security class 2 and 3 and to apply for register control on behalf of the operator in respect of employees or other persons participating in security sensitive activities.

More active supervision (and less guidance)?

The protective security supervision that previously has been essentially advisory and supportive can now be expected to change in nature to a more disciplinary supervision. This means that the SFSA can be expected to focus on supervising whether operators are compliant with the protective security legislations and, if not, impose sanctions. We have noted that the SFSA is strengthening its resources to carry out an adequate supervision and has also decided on new regulations with regard to protective security.

Yet, the Government has previously emphasised that it is the task of the supervisory authority to help operators, through regulations, recommendations and guidance, in their work with e.g. assessing whether they are covered by the Security Protection Act, when security protection agreements are to be drawn up and how security protection analyses are to be conducted.[4] This is also evident from the Protective Security Ordinance which states that the supervisory authorities shall provide

[2] Prop. 2020/21:194, p. 74 ff
[3] Chapter 8 Section 1 in the Protective Security Ordinance (2021:995)
[4] Prop. 2020/21:194, p. 76 ff

guidance on protective security within their respective supervisory areas.[5]

Our experience is that this type of advisory role does not directly correspond to the SFSA's regular role in other areas of supervision, where the authority is not always particularly inclined to provide guidance. It is therefore not clear exactly how the SFSA will design supervision in the area of protective security. One could however expect that it will differ from the supervision methodology in the SFSA's traditional areas, the question is however to what extent.

The SFSA's new regulation

The SFSA's new regulation[6] (the "Regulations") aim to streamline the authority's supervision of the operators and at the same time facilitate for the operators to fulfil certain obligations under the protective security framework. The Regulations apply to operators that conduct security sensitive activities according to the Protective Security Act and that are part of the SFSA's supervisory area. The Regulations enters into force on December 1st 2022.

According to the protective security framework, operators are obliged to notify

[5] Chapter 8 Section 12 in the Protective Security Ordinance (2021:995)
[6] The Swedish Financial Supervisory Authority's Regulations on Protective Security, FFFS 2022:17

various circumstances to the supervisory authority, and it is the practical aspects of those obligations that the Regulations deal with. According to the Regulations, an operator must use a specific form provided by the SFSA for the following purposes:

- Notification that an operator is conducting security sensitive activities or that the security sensitive activities have ceased.
- Notification that the operator intends to enter into a security agreement.
- Notification of joint consultation.
- Request for a decision on placement in a security class.

To conclude
Sweden has strengthened its regulatory framework on protective security and since the end of last year the SFSA is the authority responsible to focus specifically on the compliance level of those operators that conduct security sensitive activities in the financial sector.

It will indeed be interesting to learn how the SFSA takes on the supervisory role in this new field and to what level there will be room for guidance when the supervision can be expected to change to more disciplinary in nature. One should not expect less than that the SFSA will approach its new assignment with the greatest sense of responsibility and take an active role as a supervisory authority. We know being regulatory compliant is of greatest importance to the concerned companies. It is therefore of great importance that banks, financial infrastructure companies and other operators that may be in scope of the Protective Security Act carefully analyse whether they conduct security sensitive activities and, if they conclude they do, take appropriate actions including ensuring that they follow pertinent legal requirement and keep up to date with the SFSA's guidance.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Hanna Salajin
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

malmo@setterwalls.se