SETTERWALLS

Fintech Report 2024

SETTERWALLS

Is the regulatory tsunami we now see within the FinTech sector sustainable?

In the past, FinTech lawyers primarily focused on negotiating deals and drafting complex contracts in the emerging technology sector now known as FinTech. However, over the last decade, there has been a noticeable shift in focus. Increasingly, more time is now being spent providing guidance and navigating the often intricate surrounding regulatory landscape. Regulatory questions and issues frequently become significant obstacles or dealbreakers if not properly addressed and resolved. Additionally, many of the regulatory framework and legislation currently in place is relatively new, meaning that the sector has not yet had the opportunity to establish standard practices or common interpretations of these rules. This often results in time-consuming and costly processes.

The question we must ask ourselves is whether the regulatory burden on the FinTech sector and its innovative entrepreneurs is sustainable or overly burdensome. In my opinion, it is too early to definitively answer this question. However, we have learned that with sensible regulation, implementation, and interpretation, sustainability can be achieved over time. Currently, the delicate balance between fostering innovation, ensuring effective oversight, protecting customers, maintaining market stability, AND leveraging digital innovation opportunities is indeed a terror balance. We may therefore be in a situation where over-regulation or inadequate implementation and interpretation of rules hinder transparency for all stakeholders. We should anticipate further regulations, guidance and case law that could either boost or limit the FinTech market in the near future.

As a consequence of these observations, we have chosen to highlight some hot topic regulatory issues and trends in this year's FinTech Report 2024. Our aim is to provide guidance within the regulatory field based upon our daily work experiences with the FinTech industry.

Without further delay, it is our pleasure to present to you Setterwalls' FinTech Report

Yours sincerely,

Joacim Johannesson
Partner, and Head of Setterwalls' FinTech team

What About the Little Guy – the SME's Practical Guide to DORA

You would be hard-pressed to find anyone in the FinTech industry who hadn't noticed the buzz around DORA. Part of the success be-hind DORA's awareness campaign can probably be ascribed to the ever-increasing number of cybersecurity incidents which have sent shockwaves throughout the industry. One can only speculate about just how many further incidents have occurred but which have never surfaced. Although cybersecurity has been prioritised by legacy enterprises over the last couple of years, many smaller businesses now struggle to fulfil the requirements set by DORA. If this sounds all too familiar, then this guide is designed for you.

Background

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("**DORA**"), is part of the EU's Digital Decade strategy. The Digital Decade strategy covers many important subjects, varying from AI to cybersecurity, where DORA makes out the blueprint for cybersecurity within the financial sector and is expected to affect more than 22,000 financial entities and information and communication technology ("**ICT**") service providers in the EU.

DORA entered into force on 16 January 2023 but will not apply until 17 January 2025, effectively giving the entities affected by the regulation two years in order to comply. However, the cybersecurity trend has existed within legacy enterprises, which typically are made up of larger banks, since long before 2023. Now, we see that such legacy enterprises already have come a long way in their DORA compliance. In contrast to this, a trend can be spotted where small and medium-sized enterprises ("**SMEs**") – which generally are more streamlined, with nimble structures typically featuring low staff headcount and limited resources – oftentimes lack a clear strategy on how to tackle compliance when faced with a vast set of requirements.

This practical outcome, where legacy enterprises are able to comply, but SMEs have a hard time keeping up, has long been anticipated and is in line with criticism typically levied towards DORA. Regardless of whether such criticism is justified or not, the fact remains that SMEs must comply with the requirements imposed by DORA, in the same way that legacy enterprises must comply.[1] This raises the fundamental question; how does an SME get started? In this article, we will explain the key takeaways from DORA and provide a plan as to how to get started, which is specifically tailored for an SME audience. The guide can also be used by service providers, effectively giving insights as to how DORA will affect their respective businesses.

"This practical outcome, where legacy enterprises are able to comply, but SMEs have a hard time keeping up, has long been anticipated and is in line with criticism typically levied towards DORA."

1 Please note that some financial entities are exempted or subject to a lighter version of DORA, see Step one – Find out if, and to what extent, DORA is applicable.

Key takeaways from DORA

In essence, DORA can be summarised into the following five pillars, each of which vary significantly in their respective requirements: (1) ICT risk management framework; (2) Management and reporting of ICT-related incidents; (3) Digital operational resilience testing; (4) Management of ICT third-party risks; and (5) Information exchange arrangements.

The DORA framework contains both practical and administrative elements. Some of the more practical elements involve the establishment of backup systems, mechanisms to promptly detect anomalous activities, and the implementation of a digital operational resilience testing programme. The more administrative elements include the drafting and regular review of a potentially quite extensive set of documentation.

Although DORA is a new framework, some of the financial entities may already be familiar with the so-called EBA Guidelines.[1] At a first glance, the frameworks share several similarities, meaning that the entity, in practice, will not have to start from scratch. However, this also means that many SMEs – which have not been subject to the EBA Guidelines – may again find themselves working uphill with little to no prior experience with similar frameworks, such as the EBA Guidelines. Here, some words of comfort for the SMEs which have to start from scratch, is that DORA covers several additional, and sometimes new, aspects which go even further than the EBA Guidelines.[2]

When navigating DORA, it is important to remember that Article 4 contains a proportionality principle which states that the size, overall risk profile, and the nature, scale and complexity of the services, activities and operations shall be considered in various sections of DORA. Basically, this means that the competent authorities will likely not expect the same level of results from an SME as they would from a legacy enterprise. Finally, it should also be mentioned that some articles in DORA contain specific exceptions for financial entities meeting the definition of a microenterprise.[3]

2 EBA Guidelines on ICT risk and security risk management EBA/GL/2019/04.

3 This is especially apparent when comparing the sheer number of pages, where the EBA Guidelines makes up for 29 pages, compared to DORA's 79 pages .

4 "Microenterprise" means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million, DORA, Article 3, point (60).

The SME's "step-by-step" plan

There are several different ways and various strategies to deploy, as to how to take on the requirements imposed by DORA. In the following, we will provide one way on how to efficiently establish a foothold, and also give you some key insights along the way.

Step one* – *Find out if, and to what extent, DORA is applicable

Step one may almost come across as redundant, but it is worth having an extra look as to *if*, and *to what extent*, DORA is in fact applicable to your company. In Article 2(1), a list with over 20 different entities falling under the scope of DORA can be found. Here, it should be noted that ICT third-party service providers[4] (hereinafter "**Providers**") are not subject to the same requirements under DORA as a financial entity, meaning that DORA will only have an indirect effect on such Providers. This indirect effect will mainly occur through the contractual arrangements between the Provider and the financial entity.[5]

Under certain specific circumstances, DORA does not apply to managers of alternative investment funds. Furthermore, DORA also contains an exception whereby certain financial entities – which fall under the scope of DORA – are exempted from the "full version", meaning that such entities can enjoy a lighter and more agile version of DORA. With this being said, the exceptions are both few and quite narrow, meaning that many financial entities are likely to be subject to the full and complete version of DORA. Finally, so called *microenterprise*s are also subject to fewer and/or lighter requirements under DORA.[6]

Step two* – *Gather the team

In practice, DORA will involve many different areas and functions in your company, making it impossible for only a selected few individuals to tackle the challenge themselves. Considering this, it is crucial to gather a broad team with varying expertise in order to achieve all of the requirements under DORA. Naturally, many of the requirements will involve stakeholders within the security field, which is precisely why a few extra sets of hands are recommended in order to avoid an unnecessarily high burden for a few individuals, as well as to avoid the creation of any avoidable bottlenecks in the project.

Step three* – *Start doing a GAP analysis

Once the team is set, it is time to take the first steps towards compliance. Here, the financial entity may choose several different routes in order to reach compliance, where one quite straightforward way is to start with a GAP analysis.

If the financial entity chooses to start with this approach, the GAP analysis should contain all of the specific requirements under DORA, where mapping out such requirements can be a daunting and very time-consuming task. However, mapping out the requirements is essential in order to avoid any requirements falling between the cracks. To note also that the exercise itself also provides valuable insights in regards to what is to be expected,

5 Where an ICT third-party service provider is "an undertaking providing ICT services", and ICT services means "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services, DORA, Article 3, points (19) and (21).

6 It should be noted that a limited number of Providers will also be classified as critical Providers, meaning that the critical Provider, to a certain extent, will be subject to some requirements under DORA,

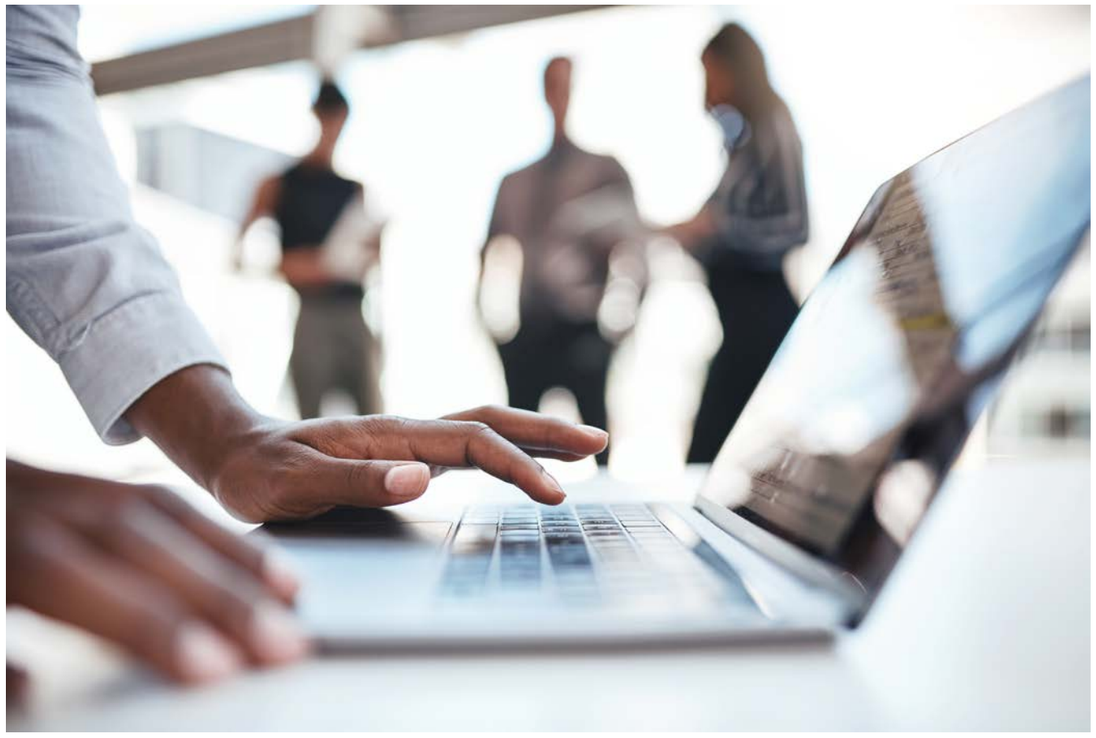
7 According to Article 3(60) DORA, a microenterprise means a "financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million".

and which functions, documents and routines are already in place (and which are not). In addition to the GAP analysis having a quality control function, it can also have the dual purpose of being a working document. By adding supplementary columns – e.g. columns covering who is being assigned the specific requirement, progress, and deadlines – an overview in a format which the stakeholders should already be quite familiar with can be achieved.

After the GAP analysis document has been drafted, each team member should be assigned with a specific set of tasks. The stakeholder should then proceed with mapping out which documentation, procedures and similar are already in place, or if additional work is required. Most likely, the result of the GAP analysis will probably differ across various financial entities, whereby some may find that they have certain necessary documentation and routines already in place, whereas others may find themselves a little bit further behind.[7]

When conducting the initial GAP analysis, it is important to keep in mind that the underlying purpose – at this stage – is to simply perform a status-check over *what is in place* and *what is lacking*.

7 By way of example, a financial entity which has been subject to the EBA Guidelines should, in theory, already have certain documentation and procedures in place.



Step four* – *Map out your ICT

In parallel with the GAP analysis, you should also start with the mapping of your existing ICT. The mapping of the ICT is, again, a potentially daunting task which will be time-consuming and require input from large parts of the organisation. Some other difficulties regarding the mapping are that it is spread out across DORA.

One extensive Article covering such mapping requirements is Article 8. Under this Article, a financial entity shall for example identify, classify, and document all (i) ICT supported business functions, roles and responsibilities; (ii) the information assets[8] and ICT assets[9] supporting those functions; and (iii) their roles and dependencies in relation to ICT risk[10]. However, several additional mapping requirements apply under Article 8, such as:

- **cyber threats[11] and ICT vulnerabilities[12];**
- **network resources and hardware equipment (including those on remote sites) and the mapping of those considered critical;**
- **the configuration of the information assets and ICT assets and their links and interdependencies;**
- **processes that are dependent on Providers and interconnections with Providers that provide services that support critical or important functions.**

In contrast to Article 8, which covers a very broad angle, Article 28(3) instead covers the requirement of a register of information in relation to all contractual arrangements on the use of ICT services from Providers, bearing some resemblance with the registers under GDPR.

Step five* – *Start with the low-hanging (and important) fruit

By this stage, you should have gained a strategic overview and already be well on your way forward. As with every project, it is important to keep moving forward and to not get too tied up in the starting pits. Here, an effective strategy could be to start with the low-hanging fruit and trust your instincts. If you already know some of the pressure points in your company's DORA compliance, then trusting your instincts with those specific problems could be a good starting point. Afterall, you know the strengths and weaknesses of your company best.

Step six* – *Start re-negotiating the ICT agreements

As stated earlier, the "DORA-effect" will inevitably spill over to the Providers, having an indirect effect on the Providers.

8 By way of example, a financial entity which has been subject to the EBA Guidelines should, in theory, already have certain documentation and procedures in place.
9 "Information asset" means a collection of information, either tangible or intangible, that is worth protecting, DORA, Article 3, point (6).
10 "ICT asset" means a software or hardware asset in the network and information systems used by the financial entity, DORA, Article 3, point (7).
11 "ICT risk" means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment, DORA, Article 3, point (5).
12 "Cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons, Regulation (EU) 2019/881, Article 2, point (8).
13 "Vulnerability" means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited, DORA, Article 2, point (16).

As for now, most legacy enterprises have started negotiating their respective agreements with the Providers, but more financial entities are expected to start doing so during the upcoming months. In order to position yourself at the front of the queue, now is a good idea to be proactive and reach out to your Provider.

The process between the financial entity and the Provider can vary and be handled differently. Many Providers will likely have their own template covering the requirements under DORA. This is due to the fact that Providers will most likely have to re-negotiate a large number of agreements, making bespoke agreements in different templates (or accepting the financial entity's own template) which is somewhat of an administrative impossibility.

If you are not in a position to insist upon having your own template, it is especially important that you make sure that the Provider's template contains all of the key contractual provisions outlined in DORA.[13]

As an ending note regarding the agreements, financial entities may, among other requirements, only enter into contractual arrangements with Providers that comply with appropriate information security standards, with the bar set even higher if the arrangement is subject to "critical or important functions". A good indicator as to whether the Provider fulfills such requirements could be that the Provider holds an ISO 270001 certification, but other factors are relevant too. Keep in mind that you are ultimately responsible for complying with all of the requirements under DORA, and not the Provider. As a consequence, it important that you properly evaluate not only the ICT agreement with the Provider, but also the Provider itself.

Ending notes

At a first glance, DORA compliance will most likely come across as a daunting task with its vast set of requirements involving many different functions, and where there are few available templates for compliance at this stage.

Here, our best advice going forward is to take a look at the bigger picture, *what is important?* The answer probably lies in the name of the regulation, digital operational *resilience* for the financial sector. The regulations concern identifying exposure, risk and deficiencies, and then working to resolve these issues, and to improve overall resilience; or as stated in the preamble, "*observing basic cyber hygiene*".[14] Once the GAP analysis and

14The key contractual provisions can be found in DORA, Article 30, where Recital (71) and (72) offers a summary.
15 DORA, Recital 13.

Niklas Follin
PARTNER
STOCKHOLM

Joel Kokko
ASSOCIATE
STOCKHOLM

Liability, Opportunity and Risk: The Use of Generative AI in the Finance Industry

The finance industry is no stranger to new technological breakthroughs, which typically come at such speed and with such ferocity that life is never quite the same again thereafter. The finance industry is yet again on the verge of another radically transformative era, with the evolution of generative artificial intelligence ("AI"). In its current iteration, AI already offers tools capable of everything from automating routine tasks to enhancing decision-making processes, and creating new strategies. These opportunities are indeed tempting, and businesses who are late to the AI game may be left behind competitors. However, implementing generative AI also comes with significant risks and liability concerns that must be carefully navigated.

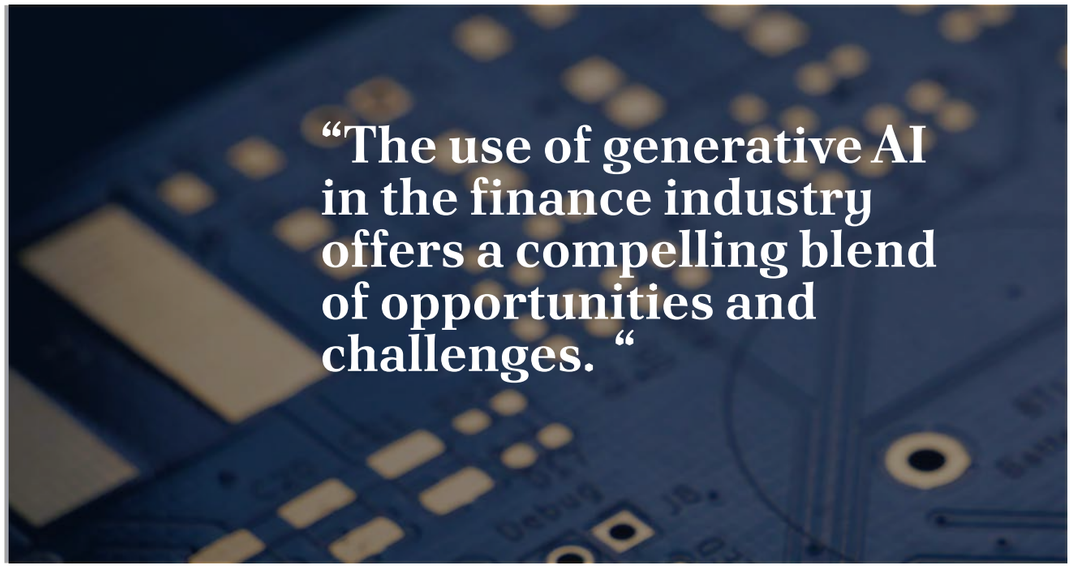
Opportunities Presented by Generative AI

Automation of Financial Reports and Analysis: Generative AI can automate the creation of financial reports, executive summaries, and personalised investment insights. This not only increases efficiency but also allows financial analysts to focus on more strategic tasks.

Personalized Financial Services: By leveraging generative AI, financial institutions can offer highly personalised services to their clients. AI can generate customised investment strategies, risk assessments, and even financial advice tailored to the individual needs of customers.

Fraud Detection and Prevention: Generative AI can be trained to identify patterns indicative of fraudulent activity. By analysing transactions in real-time, AI systems can flag anomalies and prevent potential fraudulent activity before it even occurs.

Algorithmic Trading: AI algorithms can generate predictive models that drive algorithmic trading strategies. These models can process vast amounts of market data to identify trading opportunities that may be invisible to human analysts.



Risks and Liability Concerns

Model Risk and Transparency: The complexity of generative AI models can lead to a lack of transparency, making it difficult to understand how decisions are made. This ‘black box’ issue can pose significant model risks, especially if the AI generates erroneous or biased outputs. The lack of transparency as well as the tendency for Generative AI to ‘hallucinate’ poses difficulties for financial institutions and their ability to demonstrate security and accountability, and thereby ensure regulatory compliance.

Regulatory Compliance: As financial institutions adopt generative AI, they must ensure that their use of the technology complies with existing regulations. This includes everything from the strict requirements in DORA and NIS2 regarding cybersecurity as well as the EU AI Act, but also more mundane legal requirements on everything from job application discrimination, ensuring the accuracy of generated reports, use of third-party intellectual property rights (either in the prompting phase or as part of the generated result), etc.

Data Privacy and Confidentiality: Generative AI requires access to large datasets, which may include sensitive personal and financial information. Ensuring the privacy and security of this data is paramount in order to prevent breaches that could lead to significant liability issues.

In relation to prompting and sharing information as a financial institution or from third parties (e.g., customers, trusted partners, or suppliers), many AI tools have features and/or legal terms that mean that the provider of the tool has access to and uses such information to, for example, further develop and improve the tool or other services. This may mean that the instructions become available both to the provider of the tool and other unauthorized third parties, despite and in breach of strict confidentiality undertakings by the financial institution.

Navigating the Balance

To harness the benefits of generative AI while simultaneously mitigating the associated risks, financial institutions must adopt a balanced approach.

Governance Framework: Establishing strong governance frameworks will help manage the risks associated with generative AI. This includes setting clear policies for model development, validation, and deployment but also for the purchase of third-party AI tools and their use within the organisation – including when and how employees may use confidential information and personal data when prompting an AI tool. A multi-level and cross functional approach is imperative to ensure that all actors are aware of their roles and responsibilities, and to ensure compliance with applicable law (e.g., the EU AI Act) and other legal obligations undertaken by the financial institutions (e.g., as part of a collaboration agreement with a supplier).

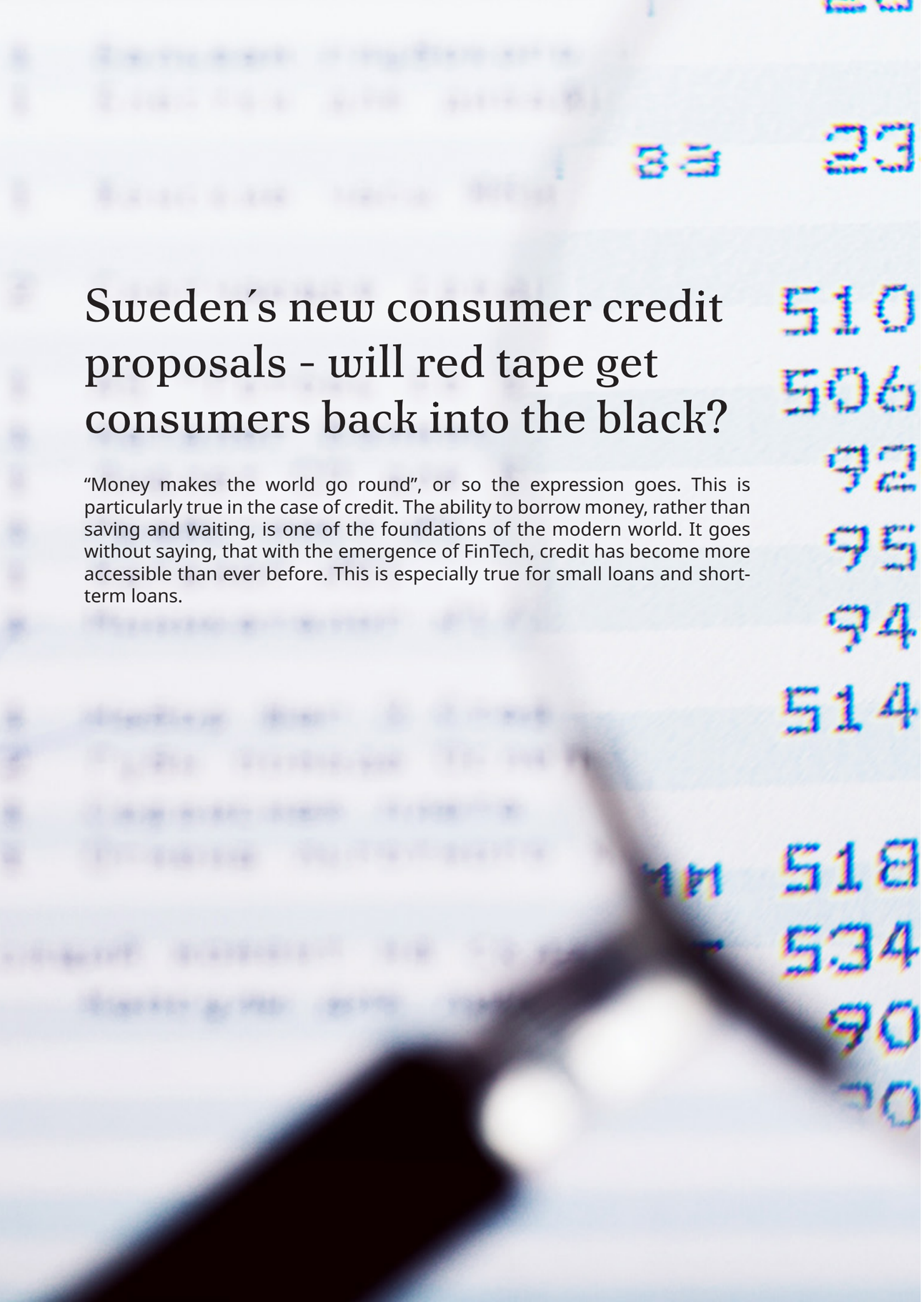
Review of Legal Terms: Generative AI tools are software programs under legal terms often supplied by the provider of the tool. To understand the risks with a specific tool, and to mitigate such, all financial institutions need to implement routines for the review of applicable terms and conditions of all third-party AI tools.

Conclusion

The use of generative AI in the finance industry offers a compelling blend of opportunities and challenges. Financial institutions that successfully integrate this technology can reap significant rewards in terms of efficiency, customer satisfaction, and competitive advantage. However, they must also be vigilant in addressing the risks and regulatory considerations that come with it. By implementing robust risk management practices in the form of inter alia governance frameworks and routines to review legal terms regulating use of generative AI by the organisation, the finance industry can navigate the complexities of generative AI and savour its opportunities with minimal risks.

Fredrik Roos
PARTNER
GÖTEBORG

Emily Svedberg-Possfelt
SENIOR ASSOCIATE
GÖTEBORG



Sweden´s new consumer credit proposals - will red tape get consumers back into the black?

“Money makes the world go round”, or so the expression goes. This is particularly true in the case of credit. The ability to borrow money, rather than saving and waiting, is one of the foundations of the modern world. It goes without saying, that with the emergence of FinTech, credit has become more accessible than ever before. This is especially true for small loans and short-term loans.

Introduction

Small, unsecured loans are primarily provided by Consumer Credit Institutions. There are approximately 70 Consumer Credit Institutions in Sweden, about 20 of which exist only to intermediate consumer loans. They are now, together with the consumer credit market as a whole, facing an even stricter regulatory environment, as the Swedish government proposes to strengthen consumer protections and tackle consumer over-indebtedness.

The proposed new measures include limited tax deductibility for consumer credit interest and stricter rules for the marketing of consumer credits, as well as new regulatory requirements.

In May 2024, the Swedish government put forward a memorandum with proposals to strengthen consumer protections on the consumer credit market and decrease private over-indebtedness. In short, the memorandum proposes to repeal the Certain Consumer Credit-related Operations Act (2014:275) (Sw. Lag om viss verksamhet med konsumentkrediter).[1] With the new rules – which are proposed to come into force on July 1, 2025 – Consumer Credit Institutions would need to be authorised as credit institutions in accordance with the Banking and Financing Business Act (2004:297).[2]

Consumer Credit Institutions can today be licensed to provide and or mediate credit to consumers. The proposal would increase the regulatory requirements for consumer credit providers seeking authorisation as well as increasing the costs and compliance requirements for anyone that wishes to provide consumer credit.

1 FiDep, dnr 2024/01078, p. 4.
2 FiDep, dnr 2024/01078, p. 30 f.

”Around 30 per cent of borrowers from Consumer Credit Institutions receive payment reminders, compared to just 5 per cent of borrowers from major banks.”

Background to the proposal

As access to consumer credit has increased, so too have the cases where borrowers have been unable to repay their loans. Generally speaking, loans provided by Consumer Credit Institutions are not only smaller and shorter-term than those provided by banks; they also have higher interest rates. Loans without collateral account for more than five per cent of total borrowing in Sweden, and represent more than 20 per cent of total interest payments.[3] Consumer Credit Institutions’ median interest rates for unsecured loans are 39 per cent, compared to 4.9 per cent for bank loans.[4]

According to the Swedish Financial Supervisory Authority (Sw. Finansinspektionen) (SFSA), borrowers with Consumer Credit Institutions generally have lower incomes and are less likely to be able to repay their debts. Around 30 per cent of borrowers from Consumer Credit Institutions receive payment reminders, compared to just 5 per cent of borrowers from major banks.

The SFSA has also studied the differences in credit assessments between Consumer Credit Institutions and banks, and found that banks are generally more prone to conduct credit and risk assessments.[5] For consumer loans of less than SEK 5000, where Consumer Credit Institutions

3 SFSA, Swedish Consumer Credit, FI Ref. 22-32666 (2022).
4 Swedish Consumer Credit, p. 34 (2022).
5 FiDep, dnr 2024/01078, p. 26.

are the most common type of lender, a discretionary income calculation is conducted in less than 10 per cent of cases.[6]

Current state of play

The Certain Consumer Credit-related Operations Act was enacted in 2014, before which Consumer Credit Institutions did not need authorisation by the SFSA. The Act meant that Consumer Credit Institutions became subject to similar rules as other financial institutions, regarding compliance, and shareholder and management suitability.[7]

Under the current rules, an undertaking that wishes to become an authorised Consumer Credit Institution must have founding documents compliant with regulations, as well as fit and proper shareholders, board members and management.

Like banks, Consumer Credit Institutions must have sound business practices.[8] An institution has a responsibility to maintain public trust in the credit market[9], and must also take their customers, and especially consumers, into due consideration.[10]

The soundness requirement is clarified in the SFSA's regulations. A Consumer Credit Institution must have written internal rules on lending that clearly specify when decisions can be taken, and which include credit limits, procedures for conducting credit assessments in accordance with the Consumer Credit Act (2010:1846), how loans are to be monitored and how the credit provider intends to manage defaulted credits.

The Consumer Credit Act also contains an interest ceiling for high-cost credit products, which the government has also proposed to decrease from 40 percentage points above the reference rate to 20 per cent.[11] The Act also requires moderation in the marketing of credit products.[12]

6 FiDep, dnr 2024/01078, p. 29.
7 Section 6 of the Certain Consumer Credit-related Operations Act.
8 Section 12 of the Certain Consumer Credit-related Operations Act.
9 Government Bill 2013/14:107 p. 51.
10 Government Bill 1992/93:89 p. 153 f.
11 Section 19a of the Consumer Credit Act. For the proposed changes, see Government Bill 2024/25:17 p. 13 ff.
12 Section 6a of the Consumer Credit Act.

> "Various stakeholders have expressed concern about the proposed regulatory changes, especially in relation to entities only intermediating consumer loans. For instance, the SFSA has criticised the lack of an impact assessment regarding consumer credit intermediaries."

Future regulatory burden

As previously mentioned, the government's memorandum proposes the repeal of the Certain Consumer Credit-related Operations Act and requires Consumer Credit Institutions to seek authorisation as banks or credit market companies. This would mean much stricter regulatory requirements, for instance, capital and organisational requirements becoming applicable to the credit provider's operations.

The added authorisation and supervision requirements would drive up the costs for consumer credit providers, and would force them to not only provide consumer credits, but to also receive funds from the public. Consumer Credit Institutions, which are today only mediating loans, would be particularly harshly affected by the proposals, as they currently neither receive funds nor provide consumer credit themselves.

The increased regulatory requirements and costs could potentially increase the entry thresholds on the consumer credit market, and lead to lower levels of competition, higher compliance costs and higher costs for the consumer. The proposed regulatory changes could also limit access to small and short-term credit.

Various stakeholders have expressed concern about the proposed regulatory changes, especially in relation to entities only intermediating consumer loans. For instance, the SFSA has criticised the lack of an impact assessment regarding consumer credit intermediaries.[13]

It should also be noted that many of the supposed issues with consumer credits, such as risk assessments and high interest rates, are regulated in the Consumer Credit Act

13 FI dnr. 24–13477, p. 4.

(2010:1846) rather than in the Certain Consumer Credit-related Operations Act. The Consumer Credit Act (also) requires sound lending practices, and moderation when marketing credit products. The Swedish Bar Association notes in its response to the government's proposal that the Consumer Credit Act does not make any difference between credit institutions and Consumer Credit Institutions.[14] The government's impact assessment does not specify how revoking the Certain Consumer Credit-related Operations Act would decrease over-indebtedness.

Conclusions

The proposed increased regulatory requirements risk creating an environment where the increased costs and barriers of entry to the consumer credit market limit competition, leading to credit becoming less accessible to consumers. The requirement for any Consumer Credit Institution to become a bank or credit market company would make many current providers untenable, and therefore decrease the numbers of FinTech startups in the consumer credit market.

It is also uncertain whether the repeal of the Certain Consumer Credit-related Operations Act would be an efficient and proportionate response to the issue of over-indebtedness. Consumer Credit Institutions are already required to observe sound lending practices, and there are multiple regulations related to consumer loans. Many of the government's proposals to strengthen consumer protections take aim at the loans themselves and the marketing of consumer credit.

Generally, major interventions in Swedish national law (which are not based on EU law common for all member states), also risk weakening Stockholm's position as one of Europe's major FinTech hubs.

As the rest of Europe is waking up to competitiveness issues, Sweden is planning to impose new regulatory requirements on many thriving FinTech businesses. Many of the proposals to combat over-indebtedness have been welcomed by the credit providers themselves, but repealing the Certain Consumer Credit-related Operations Act would lead to an entirely new regulatory environment, without addressing the root causes of over-indebtedness. Functioning financial markets require competition and innovation, rather than increased entry barriers for startups and SMEs.

The Swedish government is expected to continue its legislative work, and refer a legislative proposal to the Council on Legislation during the autumn term. However, it yet remains to be seen whether it has listened to the critique of its proposals.

14 Swedish Bar Association, R-2024/1037, p. 2.

Tobias Björklund
SPECIALIST COUNSEL
STOCKHOLM

Victor Nilsson
ASSOCIATE
STOCKHOLM

The Swedish Dilemma: Balancing Data Protection and Background Checks in the Financial Sector

The fulfilling of employee due diligence and know-your-customer obligations in the financial sector is a cumbersome exercise that needs to be reconciled with data protection, individual privacy and local legislation. In Sweden, third-party providers of background checks have been a convenient solution for many, but one that looks set to be restricted. This article aims to navigate this complex issue and explores recent Swedish legal developments.

Trust and Compliance in Financial Due Diligence

In the rigorously scrutinised finance sector, maintaining trust and integrity is paramount. Sector-specific regulations place high demands on the overall risk management and soundness of financial institutions. In addition, the last decade has been characterised by stricter requirements to verify the identity, suitability, and risks of current or potential customers under KYC and AML obligations. Such customer due diligence as well as employee due diligence is essential to prevent fraudulent transactions and maintain a reliable financial sector, with background checks being a key component for managing risks and compliance.

As high standards are set for background screening, financial actors also need to cope with complex and far-reaching data protection regulations that emphasise the privacy of the individual. How to walk this tightrope is not always addressed with the necessary clarity, not least because customer and employee due diligence and data protection requirements are governed and monitored by different regulations and supervisory authorities.

Background checks tend to be complex, time-consuming, and expensive. They necessitate expertise, dedicated internal functions, and access to pertinent information. In Sweden, financial institutions often outsource these services or use external databases for research on individuals or entities. Outsourcing has a Sweden specific benefit of *leveraging a constitutional exception to the GDPR*[1], which service providers can exploit. This has fostered a robust, though controversial, market for such services.

Legal Background: The Swedish Principle of Public Access

The Swedish constitutional laws provide for a *principle of public access to information*, which in essence means that the public has statutory access to all public documents, judgements, and decisions unless specific confidentiality applies. This provides for transparency in public affairs and decision-making, but also means that private information about most individuals is accessible. Before digitalisation, even if such accessibility was ensured by constitutional law, the accessing of substantial physical documentation was still inconvenient in practice as it required interaction with the relevant authorities in relation to virtually every document. However, now, the highly digitised government combined with the easy dissemination of information online has created a business opportunity in providing comprehensive databases of public information. At the same time, the GDPR imposes strict restraints on the processing of the personal data such documents include, especially in relation to information on criminal offences which is restricted to public authorities or as exempted by national law. However, the GDPR's impact is not as straightforward as one might think.

The Swedish Exception: Balancing GDPR with Constitutional Rights

EU legislation typically supersedes national laws. Yet, the GDPR allows member states some leeway, notably in balancing data protection with freedom of expression and information. Based on this authorisation, Swedish law exempts application of the GDPR when it conflicts with the Swedish constitutional Freedom of the Press Act or Freedom of Expression Act. Under these laws, Sweden also

1 General Data Protection Regulation (EU) 2016/679.

offers *voluntary constitutional protection* through a formal application for a so-called *publishing certificate*. Established in 2003 to accommodate new media forms and - according to its purpose - typically applying to newspapers and journalists, the obtaining of such a certificate does not require demonstrating journalistic intent and must be described as rather easily accessible.

The leeway from the application of the GDPR by way of applying for and obtaining a publishing certificate has been widely adopted by background check companies, sparking intense debate. These companies typically offer searchable online databases containing extensive personal data, such as addresses, family links, tax information, and information on criminal offences. Furthermore, their services are generally available to anyone willing to pay, leading to misuse by criminals and indiscriminate and unwarranted screening by employers. This has raised privacy concerns whilst at the same time the Swedish Data Protection Authority (IMY) has dismissed, referring to the same certificates, the flood of complaints from individuals who has felt their privacy violated by the databases.

New Developments: Shifting Legal Perspectives

Swedish courts and authorities have traditionally prioritized the freedom of the press, and thus operations protected by publishing certificates, over data protection laws. However, against the background of the rather non-journalistic purpose of several of the online databases protected accordingly, this view has recently been challenged and recent developments suggest that this position may be reversed. This year, several district courts and law enforcement authorities have refused document requests from background check companies citing a recent ruling from the European Court of Justice (CJEU), according to which public access must be balanced against individual privacy on a case-by-case basis.[2] The requesting party is thus required to display a *particular interest* in acquiring the information in order for its request to be considered legitimate.

2 Court of Justice of the European Union, C-439/19, B v. Latvijas Republikas Saeima.

IMY has now decided to investigate these new cases' implications for the handling of complaints against service providers enjoying publishing certificates.[3] The authority also presented a proposal last year for new regulations to enable financial institutions to check their customers against various sanction lists.[4] Furthermore, The Swedish government has finalized an investigation concluding that the voluntary constitutional protection through publication certificates should be amended — a topic previously examined but postponed by legislatures.[5] The new investigation proposes direct restrictions on searchable online databases of personal data.

Summarizing these developments, the winds now seem to be shifting on an issue that boils down to the principle of the primacy of EU law and the fundamental tension between freedom of expression and privacy. While investigations are underway and statutory amendments loom, a preliminary ruling from the CJEU could in itself overturn Sweden's voluntary publishing certificate system.[6] Needless to say, the future is uncertain.

3 Swedish Data Protection Authority (IMY), press release 14 May 2024, IMY competent to review search services with publishing certificates, https://www.imy.se/nyheter/imy-har-behorighet-att-granska-soktjanster-med-utgivningsbevis/.
4 Swedish Data Protection Authority (IMY), press release 18 September 2023, New rules to make it easier for some companies to handle data on offences, https://www.imy.se/nyheter/nya-foreskrifter-ska-forenkla-for-vissa-bolag-att-hantera-uppgifter-om-lagovertradelser/
5 Swedish Government, Ministry of Justice, press release 21 October 2023, Protection of personal data to be strengthened, https://www.regeringen.se/pressmeddelanden/2023/10/skyddet-for-personuppgifter-ska-forstarkas/, see also Swedish Government bill 2021/22:59, Effective protection of freedom of the press and freedom of expression.

"The potentially shifting legal landscape in Sweden is set to reshape background checks, affecting among others the financial sector."

Preparing for the Future: Adapting to a Changing Compliance Landscape

The potentially shifting legal landscape in Sweden is set to reshape background checks, affecting among others the financial sector. Potential legislative amendments and scrutiny of the system of voluntary publishing certificates, both internally and from the CJEU, indicate a future where financial institutions face an even more complex compliance environment. Such institutions may thus find their reliance on certain third-party providers more restricted, necessitating a reassessment of their internal capabilities and compliance strategies. This could burden small entities lacking the necessary resources and expertise to meet both regulatory and data protection standards. Nonetheless, the demand for third-party background check providers will persist, meaning that providers that have adapted to the new regulatory reality are likely to emerge shortly.

Financial institutions must brace for increased scrutiny of due diligence practices and a smaller margin for error in managing sensitive data, requiring a thorough understanding of e.g. the

6 Attunda District Court in case T 3743-23, decision of 1 March 2024.

GDPR. Balancing interests for background checks is tricky and identifying legal support for processing criminal data pose a particular challenge. In this context, IMY plays a crucial role as they are competent to issue authorisations for processing of such data, ensuring the financial sector's ability to perform due diligence without falling afoul of data protection laws. The IMY itself is calling for more legal clarity and has requested the government to set up an enquiry to review the need for further regulation of background checks.[7]

Conclusion: Navigating the Future of Financial Background Checks

The future of background checks in the financial sector stands at a crossroad, with sector specific regulatory compliance and data protection aspects converging. Financial institutions must be proactive in adapting to these changes, ensuring that their practices are legally compliant, ethically sound and respectful of individual privacy. By ensuring compliant internal background check functions, investigating which service providers can be relied upon, and monitoring legal developments and guidelines from regulatory authorities, financial institutions can get a flying start in the new legal environment. The financial sector's ability to navigate this new reality will demonstrate its resilience and commitment to upholding the highest standards of trust and integrity.

7 Swedish Data Protection Authority (IMY), press release 13 June 2024, *IMY calls for an inquiry on background checks,* https://www.imy.se/nyheter/imy-vill-att-det-tillsatts-en-utredning-om-bakgrundskontroller/.

Sophia Spala
PARTNER
STOCKHOLM

Ossian Johnsson
ASSOCIATE
STOCKHOLM

Drawing the Line - Managing the Overlap Between the Different Cybersecurity Regulations.

The EU's digital strategy for the internal market has led to a rise in regulatory demands on companies in recent years, with cybersecurity as a key focus area. Effective cyber protection across the EU is highly relevant given the increase in IT-related incidents and threats. However, a patchwork of regulations may lead to overlap, and impose a financial burden on companies, as well as, in the worst case scenario, counteract compliance. In this article, we will address how financial entities may manage the overlap of cybersecurity requirements imposed by the EU, and touch upon the relationship with Swedish national legislation on security in digital systems.

The EU's investment in digital governance

While several EU regulations can be considered to have an impact on the digital management of financial entities, there are some that specifically target the prevention of cybersecurity risks. The main regulation for companies in finance is the Digital Operational Resilience Act ("DORA"),[1] which will apply from January 2025. DORA covers a wide range of financial entities such as banks, insurance companies and investment firms, and includes *inter alia* provisions on operational management of information and communication technology ("ICT") risks.[2] Another regulation of relevance to the financial sector is the directive on measures for a high common level of cybersecurity across the EU ("NIS 2"),[3] which is proposed to be implemented through a new cybersecurity law in Sweden (with expected adoption during 2025).[4] NIS 2 is, in broad terms, applicable to entities which operate within specified sectors, such as banking and financial market infrastructures, and which have at least 50 employees, or have a balance sheet total or turnover exceeding EUR 10 million per year.[5] This directive imposes, *inter alia*, requirements on cybersecurity risk management measures.[6] The scope and requirements of NIS 2 are to a great extent reflected in the proposed Swedish implementation. Another EU cybersecurity regulation is the Cyber Resilience Act ("CRA"),[7] which establishes mandatory cybersecurity requirements

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.
2 See e.g. article 2 and chapter II of DORA.
3 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
4 SOU 2024:18 "Nya regler om cybersäkerhet".
5 Article 2 and Annex I of NIS 2.
6 Article 21 of NIS 2.
7 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements.

for products with digital elements that include a direct or indirect connection to a device or network.[8] The CRA enters into force on 10 December 2024 and will gradually become applicable during the following years (it will be fully applicable in December 2027). As indicated by the above description, these regulations may overlap in the context of cybersecurity.

The financial sector can thus be subject to cybersecurity requirements from several regulatory sources, which does not come without its share of challenges. The problem of overlapping regulations has been recognised by different stakeholders. The Swedish Bankers' Association has requested in a petition that the inquiry into the Swedish implementation of NIS 2 clearly clarifies that relevant provisions of the directive do not apply to banks covered by DORA. The petition recognises significant challenges for banks as more and more regulations, both EU and national, will apply to the same area.[9] Furthermore, the European Banking Federation has together with other associations released a joint statement on the duplication between CRA and DORA, which, according to them, could result in a highly complex regulatory landscape for financial services.[10] The general complexity of the EU's new regulatory landscape in different policy areas and its cumulative impact create significant challenges for companies, a fact which has also been emphasised by the National Board of Trade of Sweden in two reports published this year.[11] In broad terms, the complexity resulting from overlapping regulations will increase uncertainty, which in turn generates increased compliance costs and a high administrative burden on businesses. In the following sections, this article will discuss the interaction between the above-mentioned regulations and whether, as well as how, any overlapping areas have been addressed.

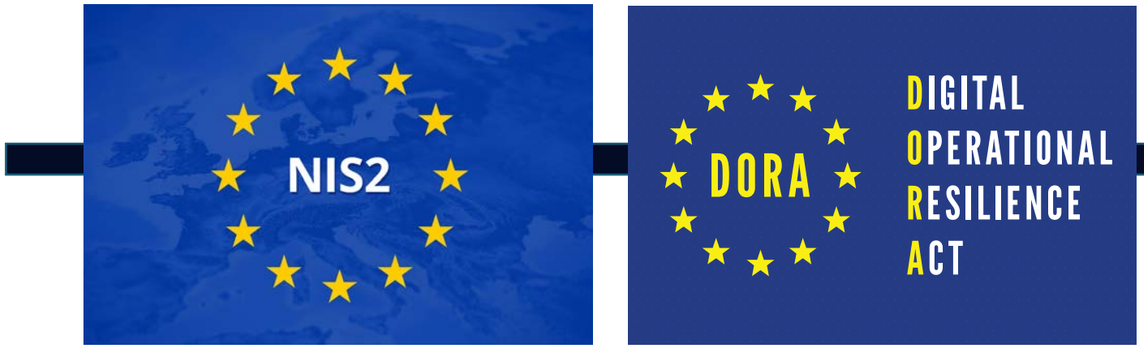
8 Article 1 and 2 of the CRA proposal.

9 See petition No. 2023/11/005 of the Swedish Bankers' Association and especially page 2 of the petition.

10 See https://www.ebf.eu/ebf-media-centre/joint-statement-on-duplication-in-the-cyber-resilience-act/ .

11 " The EU Single Market in the Digital Era – from legislative complexity to clarity" and "The Cumulative Effect of EU Regulations on External Trade – From free movement to more conditioned trade".

"Financial operators covered by DORA will not be covered by the risk management and incident reporting obligations in NIS 2, nor the supervisory and compliance control in this respect, with the consequence that they will only be subject to the obligation to notify the supervisory authority that they fall within the scope of NIS 2. "



Interaction between DORA and NIS 2

First to be analysed are DORA and NIS 2. As mentioned above, the scope of application of both DORA and NIS 2 affects various operators within the financial sector. While DORA specifically identifies the types of financial entities covered by the regulation, NIS 2 implements a more generalised approach which covers entities in certain financial sectors and of a specific size that will further have to notify the supervisory authorities if they fall within the scope.[12] Ultimately, this will result in financial institutions, such as banks, being affected by both DORA and NIS 2. Furthermore, both of these regulations impose requirements for the management of cybersecurity risks. DORA entails obligations on ICT risk management and in relation to the contractual relationship between ICT third party service providers and financial entities, while NIS 2 imposes minimum requirements on cybersecurity risk management measures, such as security in supply chain and in network and information systems acquisition.[13] It should further be noted that both DORA and NIS 2 include reporting obligations. Under DORA, major ICT-related incidents must be reported, while NIS 2 imposes reporting requirements in relation to incidents that have a significant impact on the provision of services.[14] Therefore, it can be concluded that these two regulations contain similar requirements in relation to a company's cybersecurity management.

The overlap between DORA and NIS 2 has been addressed by both the EU and in the Swedish proposal for the implementation of NIS 2. NIS 2 provides an exception for sector-specific European Union legal acts, which stipulates that where such acts impose requirements on entities to take cybersecurity risk management measures or notification of significant incidents, that are at least equivalent to the obligations set out in NIS 2, the relevant provisions of NIS 2 shall not apply to such entities.[15] DORA is identified in the recitals of the directive as such a regulation.[16] The exemption for entities affected by DORA has also been introduced in the Swedish proposal for the implementation of NIS 2, where a general exception on overlapping regulations is introduced in the draft law, while DORA is specifically identified in a draft decree that will complement the new cybersecurity law.[17] This means, in practical terms, that financial operators covered by DORA will not be covered by the risk management and incident reporting obligations in NIS 2, nor

12 Article 2 of DORA and article 2 and 3.4 of NIS 2.
13 Chapter II of DORA and article 21 of NIS 2.
14 Article 19 of DORA and article 23 of NIS 2.
15 Article 4 of NIS 2.
16 Recital 28 of NIS 2.
17 Article 9 of the Swedish proposal for a cybersecurity law.

the supervisory and compliance control in this respect, with the consequence that they will only be subject to the obligation to notify the supervisory authority that they fall within the scope of NIS 2. The clarification requested by stakeholders may therefore be considered to have been met regarding these aspects of the overlap.

Additional requirements introduced by CRA

Unlike DORA and NIS 2, which focus on organisations and the cybersecurity management of their operations, the CRA takes a different approach to cybersecurity risks, imposing requirements for security in products with digital elements. The scope of CRA will cover both hardware, such as wired and wireless products that are connected to internet, and software. Since several financial institutions as a part of their financial services offering also provide digital services in the forms of e.g., applications or platforms, entities within the financial sector, such as manufacturers or distributors of digital products, may be subject to additional cybersecurity requirements under the CRA. CRA will require products to undergo a conformity assessment process whereby several cybersecurity requirements must be met and considered in the design of products, which eventually may result in a CE marking of the product.[18] CRA further includes incident reporting obligations to authorities in addition to its security requirements. Under the CRA, manufacturers shall notify the authorities of any actively exploited vulnerability contained in digital products and any severe incident having an impact on the security of such products.[19] As indicated above, the CRA contains similar requirements to those in DORA and NIS 2.

The interaction of the CRA with other European Union legal acts, such as DORA and NIS 2, is addressed in the text of the CRA. In the recitals of the CRA, Member States are encouraged to consider providing at national level single entry points for reporting requirements, in order to simplify the reporting of information required under the CRA in consideration of other complementary reporting requirements laid down in e.g., DORA and NIS 2, as well as to decrease the administrative burden for entities.[20] Therefore, there is a possibility that the overlap in incident reporting will be

18 See for example article 13.1 and chapter III of the CRA .
19 Article 14 of the CRA.
20 Recital 72 of the CRA.

handled at the national level in a way that is more convenient for businesses. When it comes to the cybersecurity requirements on digital products in relation to operational requirements on cybersecurity in other regulations, the issue of overlap has not been clearly addressed. Instead, the position seems to be that the CRA, in relation to several aspects, complements the other legislative acts.[21] The recitals emphasise that existing European Union law on cybersecurity, such as NIS 2, does not directly cover mandatory requirements for the security of products with digital elements.[22] In the recitals, it is further stated that the CRA will facilitate the compliance with supply chain security obligations of entities that fall within the scope of DORA and NIS 2 which use products with digital elements.[23] To conclude, companies that are subject to cybersecurity requirements in other legal acts are thus not explicitly excluded from the scope of the CRA.

National legislation on security in digital systems

As financial firms may, in some specific cases, also be subject to the Swedish Security Protection Act (*Sw. Säkerhetskyddslag (2018:585)*), a brief mention should be made of this regulation. The Swedish Security Protection Act applies to security-sensitive operations, i.e., operations that are of importance to Sweden's security.[24] In the financial sector, for example, parts of the payment system and activities relating to financial stability may be of importance to Sweden's security.[25] According to the Swedish Security Protection Act, the operators affected must take necessary security protection measures, inter alia in relation to information security.[26] It should be noted, however, that the Swedish Security

21 See for example recital 24 of the CRA.
22 Recital 3 of the CRA.
23 Recital 125 of the CRA.
24 Article 1 of the Swedish Security Protection Act.
25 See https://www.fi.se/sv/bank/sakerhetsskydd/fragor-och-svar/.
26 Chapter 2 of the Swedish Security Protection Act.

Protection Act applies to operations that meet the specified criteria, not necessarily to the whole organisation. However, the same part of the organisation may fall within the scope of both DORA, NIS 2 and the Security Protection Act.[27] Nonetheless, where there is an overlap, it is only the Swedish Security Protection Act that applies. According to the Swedish legislative proposal for the implementation of NIS 2, the law will not apply to operators who only conduct safety-sensitive activities, while for operators who conduct safety-sensitive activities together with other activities, only the requirement for notification to the supervisory authority applies to the safety-sensitive part (i.e., not the requirements on risk management and incident reporting).[28] DORA further states that the regulation does not affect the responsibilities of EU member states with regard to essential state functions in the areas of public security and national security.[29] As regards the CRA, the distinction with national security legislation is not as clear, as the exemption for national security mainly applies to products that are developed or modified exclusively for national security or defence purposes.[30] To summarise, it can be assumed that (at least for DORA and NIS 2), national safety legislation will take precedence over these EU regulations.

To conclude

In summary, although the boundaries of the (yet to be formally adopted) CRA are uncertain, it is clear that the requirements of DORA take precedence over NIS 2, if one is covered by both regulations. Furthermore, the Swedish Security Protection Act will have priority in the case of security-sensitive activities. Drawing the line between these regulations will pose a significant challenge for the financial entities concerned. Hopefully this article has provided some guidance and clarity in navigating the complex regulatory landscape of cybersecurity.

27 See Fi2024/00073 on page 65 and https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/nis-regleringen-och-sakerhetsskyddslagen/.
28 See chapter 1 article 13 of the Swedish proposal for a cybersecurity law and SOU 2024:18 “Nya regler om cybersäkerhet” on page 166.
29 Article 1.3 of DORA.
30 See article 2.7 of the CRA proposal.

Niklas Follin
PARTNER
STOCKHOLM

Sofia Wahlgren
ASSOCIATE
STOCKHOLM

Scraping the Surface of Web Scraping - What Fintech Companies Should Consider When Harvesting the Web

In the highly competitive Fintech industry, staying ahead requires vigilant monitoring of competitors’ activities, customer behaviour, and up-to-date government regulations. Consequently, Fintech companies must have swift and accurate access to data, whether for optimizing investment strategies, understanding market trends, or enhancing customer experiences. Data collection and analysis are thus pivotal in this industry. This article delves into some of the regulatory requirements surrounding web scraping—a term often associated with the automated extraction of data from websites, despite its lack of a precise legal definition. While web scraping can provide valuable insights and benefits to Fintech companies, it also presents legal challenges that must be navigated carefully.

Use of scrapped date

Web scraping, also known as web data extraction or web harvesting, refers to the automated process of collecting data from websites. Scraping software tools varies in sophistication, from tools that capture the entire content of web pages to those designed to extract specific data elements. This process often involves a large-scale, indiscriminate collection of data, where the scraped data can provide profound insights and be particularly beneficial to fintech companies in areas such as:

- **Identification of customer whims and market rhythms;**
- **Financial information and other economic indicators;**
- **KYC and AML data;**
- **Training of artificial intelligence ("AI") tools and algorithms; and**
- **Market insight and social listening.**

The utilization of scraping tools on websites that are frequently visited by individuals or that contain valuable intellectual property rights ("**IPR**") can present several legal challenges. These challenges may include unlawful processing of personal data, unauthorized copying of information protected by IPR, and potential violation of agreements governing use of the website. Below we will investigate each of these legal hurdles more closely.

Processing of personal data

Personal data does not loose its protection under the GDPR simply by being published online, which means that the requirements under the GDPR must be complied with when web scraping. The European Data Protection Supervisor and several national data protection authorities have recently issued guidelines addressing the data protection risks associated with web scraping, particularly in the context of generative AI. Key concerns include the unlawfulness of the processing as well as the lack of compliance with the principle of data minimisation and transparency towards the data subjects.

In order for processing of personal data to be lawful, there must be a legal basis according to article 6 of the GDPR and the available legal basis for web scraping is in general legitimate interest. However, the use of legitimate interest requires a balancing of the rights and interests at issue to be carried out. It is the data controller who needs to demonstrate that this assessment has been performed. In some cases, a data protection impact assessment also needs to be completed. In this respect, it can be noted that the Dutch Data Protection authority has concluded that only *targeted* scraping – i.e. very limited scraping in terms of sources and purposes – is compatible with the GDPR.[1]

Furthermore, the principle of data minimisation in article 5 of the GDPR requires the data controller to not process more personal data than necessary. This can be met by for example defining precise collection criteria, ensuring that certain data categories are not collected or that certain sources are excluded from data collection, and by adopting measures to delete or anonymise personal data.[2] In this regard, it should be noted that the Swedish Authority for Privacy Protection (IMY) has categorized web scraping as a high-risk method from a data protection standpoint due to the vast volumes of data processed when using such method.[3]

Moreover, the transparency requirements towards data subjects in articles 13-15 of the GDPR mean that, as a general rule, the data controller must inform the data subjects about the processing of their personal data when the personal data is collected and when the data subject requests such information. However, a data controller that scrapes large quantities of personal data may find it challenging to appropriately inform data subjects accordingly. It may therefore in certain instances be justified to provide a privacy notice only via public means in accordance with article 14.5 of the GDPR.[4]

IPR protection

Photos, texts and other materials on websites may be protected by copyright. Under Swedish copyright law, which is harmonised to certain extent through EU acts, no formal requirements are necessary for a work to enjoy such protection. It is instead sufficient for the work to exhibit some level of originality and be the result of the creator's own efforts. This grants the creator the exclusive right to reproduce, modify, and distribute the protected work to the public. Thus, if web scraping software makes unauthorized copies of protected works, such scraping likely violates the copyright to such works. For instance, copies are created when data is collected for processing, such as aggregation and compilation, meaning that a reproduction takes place. The same data is made available to the general public when it is included in a new product available to such public or posted on a website accessible to others.

In some instances, websites may also fall under the database right protection, having

1 The Dutch Data Protection Authority, Guide to scraping by private individuals and private organisations (in Dutch), May 2024.
2 EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23 May 2024.
3 IMY report 2021:1.
4 EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23 May 2024.

the effect that web scraping may also infringe upon the rights of database producers.[5]

User agreements

Under Swedish contract law, a website user can – under certain circumstances – be bound by the terms of use of a website by the mere engaging with the website. This means that such terms may apply to the conducting of scraping operations on websites. In this regard, it has already been confirmed by a CJEU ruling that the holder of a publicly accessible database is free to impose contractual conditions on the use of its database, including provisions against scraping.[6] In this regard, it is widely common that platforms such as Facebook, LinkedIn and Bloomberg prohibit scraping and other automatic information collection on their websites via their terms of use.

In essence, if a website's terms of use prohibit data extraction, using a scraping tool in violation of such terms risks breaching the contract, which could lead to damages, injunctions preventing the use of the data, or other consequences. For example, Facebook has deleted accounts, apps, and pages from foreign companies that provided analytical services in violation of Facebook's terms of use. Accordingly, it is recommended to investigate whether the website from which it is desired to extract information offers compliant ways of doing so, such as through specific integrations and APIs.

Summary and conclusion

Web scraping may offer benefits for Fintech companies, including the ability to optimize strategies, understand market trends, and enhance customer experiences. However, it comes with complex legal challenges. To leverage its advantages while avoiding legal pitfalls, it is crucial for companies to ensure compliance with relevant regulations. This includes conducting thorough legal audits, staying updated with changes in laws and regulations, and implementing robust data protection measures.

5 CJEU, Innoweb BV v. Wegener (C-202/12).

6 CJEU, Ryanair Ltd v PR Aviation BV (C-30/14).

Sophia Spala
PARTNER
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

malmoe@setterwalls.se

setterwalls.se