FinTech Report

2026



SETTERWALLS

New rules, new reality: navigating the FinTech landscape 2026

Over the past year, the FinTech market has continued to build on the momentum we observed in 2025 — a market that had reset and was picking up pace again. That pace has carried into 2026, but the conversation has shifted. Where a year ago the focus was on whether the market was truly turning, the focus today is on how companies sustainable operate within a regulatory landscape that is no longer taking shape — it is, for the most part, already here. From the new Payment Services Package and consumer credit rules to the AI Act, the Cybersecurity Act alongside DORA, and the Cyber Resilience Act, the frameworks shaping this next phase are now a working reality.

At the centre of this shift is artificial intelligence, which continues to drive product development and reshape service delivery across the financial sector. With the AI Act entering into force, the questions surrounding high-risk AI systems are moving from the theoretical to the very practical. At the same time, the rapid development of AI is raising fundamental questions about the data that feeds these systems: the use of IPR-protected material as training data and the legal landscape around web scraping.

Navigating this evolving and often cross-border regulatory environment alongside rapid technological change remains a defining challenge for the FinTech industry. Much of the framework that was recently under debate is now in force, and the practical work of understanding how new and overlapping rules apply in day-to-day operations is well under way. Settled practices and common interpretations have yet to emerge across many of these areas, and for companies operating across borders the interplay between overlapping frameworks adds a further layer of complexity.

As a result of these observations, we have chosen to explore these themes in this year's FinTech Report. Our aim is to provide guidance within the commercial technology 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 2026. We hope you find it to be both insightful and enjoyable.



Yours sincerely,

Joacim Johannesson
Partner, and Head of Setterwalls' FinTech team

4 **The AI Act and High-Risk AI in Finance: A Practical Roadmap**
Sophia Spala & Ninorta Yohanna

10 **Mobile Banking Apps Under the CRA: Navigating Remote Data Processing Obligations for Financial Entities**
Fredrik Roos & Emily Svedberg-Possfelt

16 **The Swedish Cybersecurity Act – Where Do We Stand, And What Lies Ahead?**
Niklas Follin & Filip Liljekvist

22 **PSD3 and the PSR: A Compliance Roadmap for Swedish PSPs**
Tobias Björklund & Victor Nilsson

28 **Feeding the AI Machine – What's Legal, What's Risky, and How do You Navigate the Grey Zones**
Niklas Follin & Hanna Salajin

32 **Locked in? How the EU Data Act's Cloud Switching Rights Are Reshaping FinTech Infrastructure**
Sophia Spala & Daniel Cederquist

The AI Act and High-Risk AI in Finance: A Practical Roadmap

The AI Act is the EU's first comprehensive horizontal regulation of artificial intelligence and applies to a range of actors across the AI value chain on the EU market, from those who develop AI systems to those who use, import or distribute them. It follows a risk-based approach where certain AI practices are outright prohibited, some AI systems are classified as high-risk and subject to detailed requirements, and the rest face lighter obligations. The AI Act is currently only partially in force, with the rules on high-risk AI systems taking effect from 2 December 2027 or 2 August 2028, depending on the specific system. This article cuts through the regulatory text and offers a hands-on guide to high-risk AI systems, including the specific obligations they trigger, and the division of responsibility between the categories of actors most relevant for FinTechs: those who develop AI systems and those who use them.

When is your AI system "High-risk"?

The AI Act takes a list-based approach in its classification of AI systems. Thus, an AI system is high-risk if its intended purpose falls within one of the use cases listed in Annex III to the Act, or if it is a safety component of a product covered by the harmonisation legislation listed in Annex I, and this applies regardless of how advanced the technology of the system is. For financial services, two examples are central: AI systems used to evaluate the creditworthiness of natural persons or establish their credit score (Annex III point 5(b)) and AI systems used for risk assessment and pricing in life and health insurance (Annex III point 5(c)). Other financial AI may also be caught, depending on its purpose, e.g. automated investment advice tools or AML/KYC systems that feed into decisions about an individual.

In practice, the rules can catch a wide range of FinTech use cases: automated lending platforms, buy-now-pay-later scoring engines, credit risk models, insurance pricing and underwriting systems, and AML or KYC screening that affects an individual's access to financial services. If the system influences whether natural persons get credit, what they pay for insurance, or whether they can access a service, it may be in high-risk territory.

Article 6(3) provides an important exception. An AI system listed in Annex III will not be considered high-risk if it does not pose a significant risk of harm to health, safety or fundamental rights, including by not materially influencing the outcome of decision-making. However, this exception never applies where the AI system performs profiling of natural persons. For most credit scoring and insurance pricing use cases, profiling is inherent, which means the exception is unlikely to be available in practice.



The compliance toolkit: what high-risk actually requires

Articles 8 to 15 of the AI Act set out the requirements for high-risk AI systems. Article 8 provides the overarching principle that compliance with these requirements must take into account the system's intended purpose and the generally acknowledged state of the art on AI. Articles 9 to 15 then set out the specific requirements. They are detailed, but not unmanageable once you break them down. Here is what you are working with:

Risk management system (Article 9)

You need a documented, ongoing, iterative process for identifying, analysing, evaluating, and mitigating risks throughout the AI system's lifecycle. The risk management system must be updated as the system evolves and as new risks emerge, and should be thought of as a living document,

not a filing cabinet exercise.

Data and data governance (Article 10)

Training, validation, and testing data must be relevant, sufficiently representative, and as free from errors as reasonably achievable. You need processes for bias detection and mitigation. This matters across financial AI and the AI Act expects you to address these issues before deployment, not after.

Technical documentation (Article 11)

Technical documentation must be drawn up before the system is placed on the market or put into service, and kept up to date thereafter. It should be detailed enough for a competent authority to assess compliance.

Record-keeping and logging (Article 12)

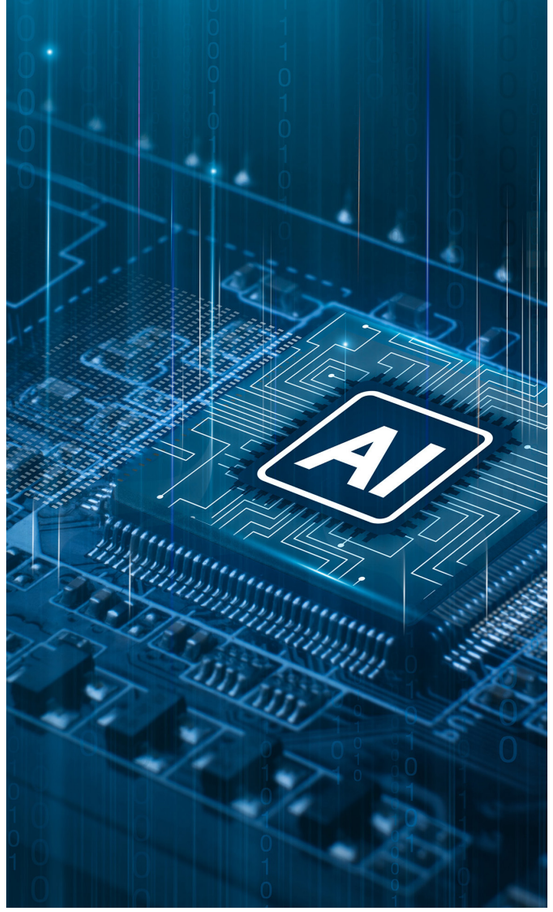
High-risk AI systems must be designed to automatically log events during operation, enough to enable traceability and review after the fact. In practice, this means being able to reconstruct why a particular decision was reached, whether that decision was, for example, to deny a loan or flag a transaction.

Transparency and provision of information to deployers (Article 13)

The system must come with instructions for use that are clear enough for the deployer to understand the system's capabilities, limitations, and intended purpose, and to interpret its outputs correctly. In plain terms, the user manual has to be genuinely useful.

Human oversight (Article 14)

The system must be designed so that it can be effectively overseen by natural persons, including the ability to override or disregard the AI's output. In short, the system cannot be a black box that makes final calls on its own, there needs to be a real possibility for a qualified person to



step in.

Accuracy, robustness, and cybersecurity (Article 15)

The system must achieve appropriate levels of accuracy, be resilient to errors and inconsistencies, and be protected against unauthorised third-party manipulation. For FinTechs already subject to e.g. DORA[1] or NIS2[2], the cybersecurity requirements should feel familiar. The trick is aligning them with what the AI Act adds rather than building parallel compliance workstreams.

Providers vs. deployers: who does what?

In addition to the requirements set out in Articles 8 to 15, the high-risk classification triggers a set of procedural and organisational obligations that are split between *providers* (those who develop or commission an AI system and place it on the market or put it into service under their own name) and *deployers* (those who use an AI system under their own authority in a professional capacity).

The provider carries the heaviest burden. This includes conducting the conformity assessment, affixing the CE marking, establishing a quality management system, maintaining technical documentation, registering the system in the EU database, and running post-market monitoring. The provider is, in effect, the party that vouches for the system's compliance before it reaches the market.

The deployer's obligations are lighter but far from trivial. Deployers must use the system in accordance with the provider's instructions, ensure human oversight is actually exercised (not just theoretically possible), monitor the system for risks during operation, keep logs as required, and, where applicable, carry out a fundamental rights impact assessment before putting the system to use. Deployers must also inform individuals when a decision affecting them has been made with the assistance of a high-risk AI system. In practice, this means that if your system is involved in, for example, denying a loan application, the person affected needs to know that AI was part of the process.

Here is where it gets interesting for FinTechs: many of you are *both*. If you develop your own credit scoring model and deploy it in your lending operations, you wear both hats simultaneously. That means the full stack of obligations applies. Even if you start as a deployer, say, licensing an off-the-shelf model from a vendor, you can be reclassified as a provider if you substantially modify the system or put it on the market under your own name or trademark. The key takeaway is to understand your role clearly, and to reassess it if your use of the system changes.

A practical roadmap: where to start

The requirements under the AI Act are detailed, but workable if you approach them methodically. The following steps are a sensible starting point, and while they do not cover every obligation under the AI Act, they address the groundwork that needs to be in place before the more formal compliance steps come into play.

1. **Inventory your AI systems and classify them.** A good starting point is to map every AI system in your organisation against the AI Act's risk categories. Focus on what your systems actually do, not what the marketing materials say.
2. **Assign roles.** For each high-risk system, work out whether you are a provider, deployer, or both. If you license AI from a third party but fine-tune or substantially modify it, you may have crossed into provider territory.
3. **Conduct a gap analysis.** For providers, this means mapping not only the technical requirements in Articles 8 to 15, but also the procedural obligations such as quality management, conformity assessment, registration, and post-market monitoring obligations. For deployers, map your operational practices against Article 26, including the potential obligation to carry out a fundamental rights impact assessment and to inform individuals subject to decisions assisted by a high-risk AI system. For both, the gap analysis should also cover baseline obligations such as transparency towards individuals who interact with certain AI systems and ensuring adequate AI literacy among staff involved in operating them.

[1] Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.
[2] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.

4. **Build or update your risk management and data governance frameworks.** If your risk management process is not yet iterative and lifecycle-oriented, this is the time to develop it. The same goes for training data governance.
5. **Establish human oversight procedures and train the people who will exercise them.** For providers, this means designing the system so that effective oversight is possible. For deployers, it means ensuring oversight actually happens in practice, assigning individuals with the necessary competence and authority, and making sure they understand the system's logic, its limitations, and when to step in.
6. **Prepare your technical documentation and logging infrastructure.** Documentation needs to be in place before the system goes live, and logging should be built in from the start. Adding traceability at a later stage tends to be significantly harder and more costly.
7. **Integrate AI Act compliance into existing structures.** Rather than building a standalone AI Act compliance programme alongside your GDPR[3], DORA, and financial regulation functions, consider integrating AI compliance into what you already have. Many of the AI Act's requirements overlap with existing obligations on data governance, risk management, cybersecurity, documentation, and oversight. Where they do, one coherent process will likely serve you better than many parallel ones.

[3] General Data Protection Regulation (EU) 2016/679.

Conclusions

For FinTechs operating in the EU, the AI Act introduces a new paradigm of accountability. Whether you are developing AI tools or deploying them, the first step is to determine your role and understand the corresponding obligations. For providers, the focus is on robust design, data quality, and transparency from the outset. For deployers, the emphasis is on responsible implementation, human oversight, and continuous monitoring. Ultimately, the AI Act mandates a partnership between providers and deployers to ensure that innovation in finance remains trustworthy, safe, and fair.



Sophia Spala
PARTNER
STOCKHOLM



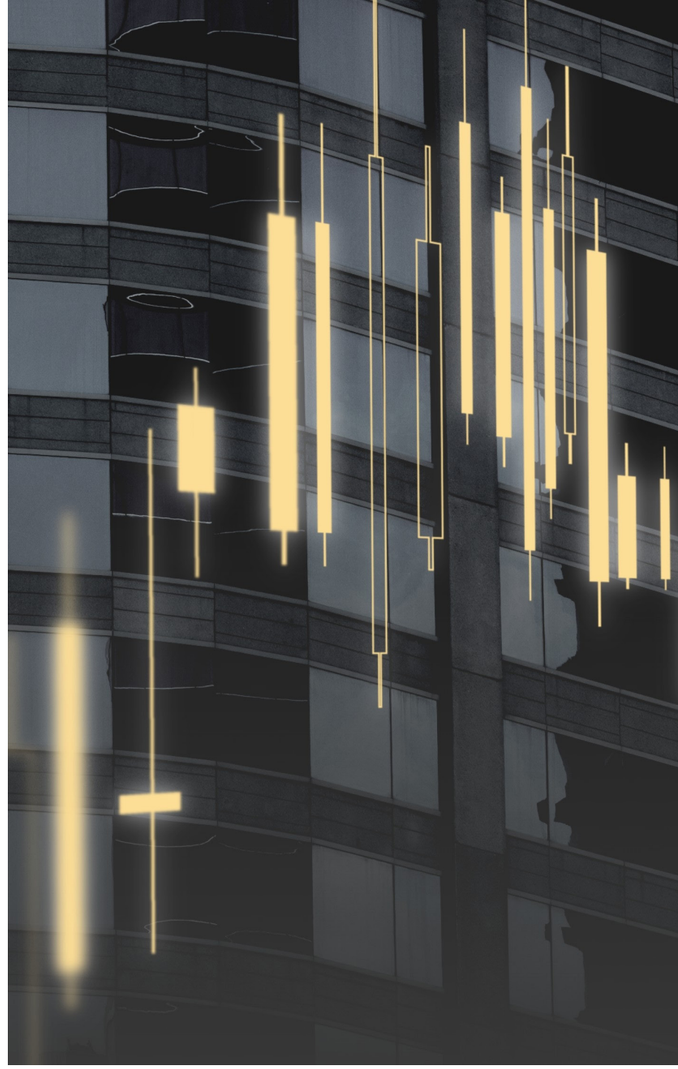
Ninorta Yohanna
ASSOCIATE
STOCKHOLM



Mobile Banking Apps Under the CRA: Navigating Remote Data Processing Obligations for Financial Entities

Financial entities are used to thinking about cybersecurity through the lens of entity-level regulation: DORA, NIS2 and supervisory expectations. The Cyber Resilience Act[1] (the "CRA") introduces a different perspective - it regulates individual products. For example, a mobile banking app published in an app store is a product with digital elements (governed by the CRA). CRA vulnerability and incident reporting requirements already apply from 11 September 2026 and the main obligations become applicable on 11 December 2027.[2] The question of where the "product" ends and the bank's wider IT estate begins has therefore become key. The Commission's Guidance on the Application of the CRA (the "Guidance") addresses precisely this question, using a mobile banking application as its first illustrative use case.[3] This article explains that use case, what it means for the boundary between in-scope remote data processing and external dependencies, and how third-party SaaS integrations should be handled. The Guidance is not binding, but it sets out the Commission's interpretation and will shape how market surveillance authorities approach compliance.[4]

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj (the "CRA").
[2] CRA, recital 126: the Regulation applies from 11 December 2027, save that the reporting obligations for actively exploited vulnerabilities and severe incidents apply from 11 September 2026 and the provisions on notification of conformity assessment bodies from 11 June 2026.
[3] European Commission, Guidance on the Application of the Cyber Resilience Act, Annex to Commission Notice C(2026) 5252, 27 July 2026 (the "Guidance"), section 8.3.1 ("Mobile banking application"). An earlier draft circulated for public consultation (3 March to 13 April 2026) contained a corresponding section 8.3.1 entitled "Banking application" (the "Draft Guidance").
[4] Guidance, para. 8. Only the Court of Justice of the European Union may give an authoritative interpretation of the CRA; the examples in the Guidance are not intended to replace a case-by-case assessment.



1. The banking app as a product with digital elements

A mobile application that a user downloads from e.g., an app store and installs on a smartphone or laptop executes on the user's device and is therefore a product with digital elements; where it is placed on the market in the course of a commercial activity, it may thereby fall within the CRA.[1] By contrast, a web application accessed exclusively through a browser is not itself a product, unless it supports the functionality of one.[2] The distinction matters for banks offering both a native app and online banking: the native app is the CRA product, and the browser-based service is relevant only insofar as it supports that product.

Crucially, the CRA defines a product with digital elements as a software or hardware product *and its remote data processing solutions*.[3] A bank cannot therefore confine its compliance analysis to the software on the customer's phone. Article 3(2) defines remote data processing as data processing at a distance for which the software is designed and developed by the manufacturer, or under its responsibility, and the absence of which would prevent the product from performing one of its functions.[4]

2. The RDPS test in brief

The Guidance reduces the definition to two decisive and cumulative questions (once processing takes place "at a distance"): (i) would the absence of the processing prevent the product from performing one of its functions; and (ii) is the software designed and developed by the manufacturer, or under its responsibility? Only if both answers are affirmative does the processing qualify as an RDPS. If the first answer is yes but the second is no, the third-party solution is to be treated like a component. If the first answer is no, the processing falls outside RDPS but its risks must still be assessed.[5]

Two limiting principles frame the test. First, recital 11 of the CRA makes clear that RDPS requirements do not entail measures to manage the security of a

[1] Guidance, section 2.1, Example 3; see also European Commission, FAQs on the EU Cyber Resilience Act (version of 3 December 2025), section 1, listing a mobile app downloadable via an app store as a product with digital elements.
[2] Guidance, section 2.1, Example 5.
[3] CRA, Article 3(1); Guidance, para. 178.
[4] CRA, Article 3(2); Guidance, paras. 180 and 184.
[5] Guidance, paras. 188–202 and the stylized flowchart at Figure 9.



manufacturer's network and information systems *as a whole*.[6] Second, the Commission expressly excludes internal systems such as HR, payroll, CRM and CI/CD pipelines, as well as security testing activities, from the notion of RDPS.[7] For a bank, this is an important signal: the CRA is not a backdoor route to regulating core banking infrastructure as a product.

3. The banking interface versus the ledger

The Commission's use case describes a financial entity that places a mobile banking app on the market, supported by self-hosted infrastructure. The customer is authenticated through a "banking interface" developed and hosted by the entity, which receives the app's requests and returns responses. That interface verifies identity by querying the account-management system and, when a transfer is initiated, submits a request to the ledger system. The account-management and ledger systems, logically segregated from the banking interface, record the transaction, and the ledger returns the status via the interface to the customer.[8]

The banking interface is an RDPS. It is necessary for the app to authenticate the customer, submit instructions and return the resulting status, and it is designed and developed under the bank's responsibility. It must therefore be included in the cybersecurity risk assessment and in the implementation of the essential requirements for the product as a whole.[9]

The account-management and ledger systems are not RDPS. The app does not interact with them directly, but only through the banking interface, and the subsequent processing of an instruction, including recording, settlement and clearing, is carried out by systems with which the app has no direct contact.[10] Notably, the final Guidance refines the reasoning of the consultation draft. The draft stated that these systems did not support one of the app's functions; the final text concedes that their availability may be necessary for a function to be completed, but anchors the exclusion in the absence of *direct interaction*.[11] This "direct interaction" criterion is now the operative boundary: RDPS is limited to the software modules responsible for the product's functionality and the interfaces those modules use with external services.[12]

For financial entities, the practical lesson is architectural. Logical segregation between customer-facing interfaces and core systems is not merely good security practice; it also helps to delimit the scope of the conformity assessment. A monolithic back end in which the app talks directly to the ledger would be harder to carve out.

4. External dependencies remain within the risk assessment

Falling outside RDPS does not mean falling outside the bank's CRA analysis. The CRA establishes two complementary obligations: a cybersecurity risk assessment for the product under Article 13(2), and due diligence regarding integrated components under Article 13(5).[13] Where risks originate outside the product, the CRA does not require the manufacturer to control or govern the external environment; it requires the manufacturer to identify those risks and mitigate them through the design of the product itself. The CRA regulates how the product responds to external risks, not how back-end infrastructure is organized, staffed or operated.[14]

The Guidance accordingly describes back-end systems as "external dependencies" that must be assessed and mitigated through product-level measures.[15] In the banking use case, compromise of the ledger could allow an attacker to influence transaction results displayed in the app. The bank must address that risk through measures such as strong authentication of back-end interfaces, integrity protection of transaction data, secure communication channels and verification of responses received by the app.[16] In other words, the ledger is out of scope, but its potential to undermine the app is very much in scope. Risk assessments should therefore map dependencies explicitly, document why each one is or is not an RDPS, and link each relevant threat to concrete controls in the app or the banking interface.

[6] CRA, recital 11, quoted in Guidance, paras. 181–182.
[7] Guidance, para. 182, which excludes, inter alia, HR, payroll, CRM and CI/CD systems, as well as penetration testing, threat hunting and red teaming.
[8] Guidance, section 8.3.1, 'Self-hosted infrastructure developed by the financial entity'.
[9] Guidance, section 8.3.1, 'Implications for RDPS', first bullet.
[10] Guidance, section 8.3.1, 'Implications for RDPS', second bullet; see also para. 205.
[11] Compare Draft Guidance, section 8.3.1 (stating that the ledger and account-management systems 'do not interact directly with the app and do not support one of its functions') with Guidance, section 8.3.1 (acknowledging that 'their availability may be necessary for a function to be completed' but limiting the CRA to parts of the system that interact directly with the product). The Draft Guidance also referred to a 'banking API layer' rather than a 'banking interface'.
[12] Guidance, para. 205. See also Draft Guidance, para. 189, noting that the intent is not to cover the entire entity's environment.
[13] CRA, Article 13(2) and (5); Guidance, section 7.3.
[14] Guidance, para. 169.
[15] Guidance, para. 206.
[16] Guidance, section 8.3.1, second bullet under 'Implications for RDPS'.

5. Third-party SaaS: chat, notifications and beyond

Modern banking apps integrate a range of third-party services. The Guidance distinguishes cloud service models: software deployed by the manufacturer on third-party IaaS or PaaS may qualify as RDPS, whereas a third-party SaaS application, offered as a fully developed product with limited configuration, is not designed and developed by or under the responsibility of the manufacturer.[17]

The use case applies this to an integrated customer-support chat built and operated by a third party. The chat is necessary for one of the app's functions but is not an RDPS. It should nonetheless be treated like a third-party component: the chat channel could be used to impersonate the bank or deliver malicious content, and the bank must mitigate those risks through product-level measures such as isolating the chat from core banking features, controlling data flows and validating content, and must exercise due diligence on the SaaS provider.[18] The same logic applies where SaaS elements are integrated in a way that affects the product's security: the manufacturer must address the risks on the product itself and exercise due diligence proportionate to the risk.[19]

The consultation draft also contained a transaction-notification example: notification logic written by the bank and deployed on a third-party PaaS was an RDPS, while the PaaS itself was to be treated like a component.[20] Although dropped from the final use case, the example remains a useful illustration of the general PaaS analysis. Banks should note that tailor-made code remains an RDPS regardless of who hosts it, since it is design and development, not operation, that is decisive.

Several practical consequences follow. The technical documentation must state that the product has RDPS or relies on third-party remote solutions and describe them.[21] Evidence of compliance with DORA, among other assurance artefacts, may be re-used in support of the manufacturer's assessment and due diligence.[22] Contracts and SLAs with third-party providers should embed security guarantees, including vulnerability handling, and require providers to notify changes, which may trigger a revised risk assessment; a major change by the provider does not, however, amount to a substantial modification of the bank's product.[23] For banks, this creates a welcome opportunity to align DORA ICT third-party risk processes with CRA due diligence rather than build parallel workstreams, although the Commission has signaled that further guidance on the CRA–DORA interplay may follow.[24]

6. Critical voices raised

It worthwhile to know that Svenska Bankföreningen (the Swedish Bankers' Association (the "**Association**")) has taken a clear position on the issue of CRA-DORA interplay/overlap. In its consultation response of 14 April 2026 on the Swedish inquiry into supplementary provisions to the CRA (SOU 2025:115), it raised no objections to the proposed national implementation but warned of overlapping and duplicative requirements in relation to DORA.[25] The Association noted that, although DORA is not a product regulation, it applies precisely to the systems through which financial services are delivered via digital channels, and is supervised by Finansinspektionen (the Swedish Financial Supervisory Authority) already. Applying the CRA on top would, in the Association's view, add complexity and cost without strengthening security, for example through parallel incident reporting to Finansinspektionen under DORA as well as to ENISA and the NCSC under the CRA.

The Associate therefore argues that financial services provided through digital channels, such as mobile banking apps, payment cards, ATMs and payment terminals, should be exempted by a delegated act under Article 2(5) CRA, which allows the Commission to exclude products already covered by Union rules offering the same or a higher level of protection. It points out that DORA covers the full lifecycle of these systems, including governance, risk management, incident and vulnerability handling and customer communication, and urges that such a delegated act be adopted as soon as possible, mirroring DORA's recognition as *lex specialis* under NIS2. Until any such exemption is adopted, however, the Commission's Guidance confirms that banking apps remain within the CRA, and financial entities should plan accordingly.

7. Concluding remarks

The Commission's banking use case offers financial entities a workable boundary: the app and the interfaces it talks to directly are the product; the ledger, account-management and wider core systems are not. Yet the boundary is one of scope, not of responsibility. Banks must still assess the risks those dependencies pose, design the app and its interfaces to withstand them, and treat integrated SaaS services as components subject to due diligence. Entities that document their architecture carefully, segregate customer-facing interfaces from core systems, and leverage their existing DORA frameworks will be well placed to demonstrate compliance before December 2027.





Fredrik Roos
PARTNER
GÖTEBORG

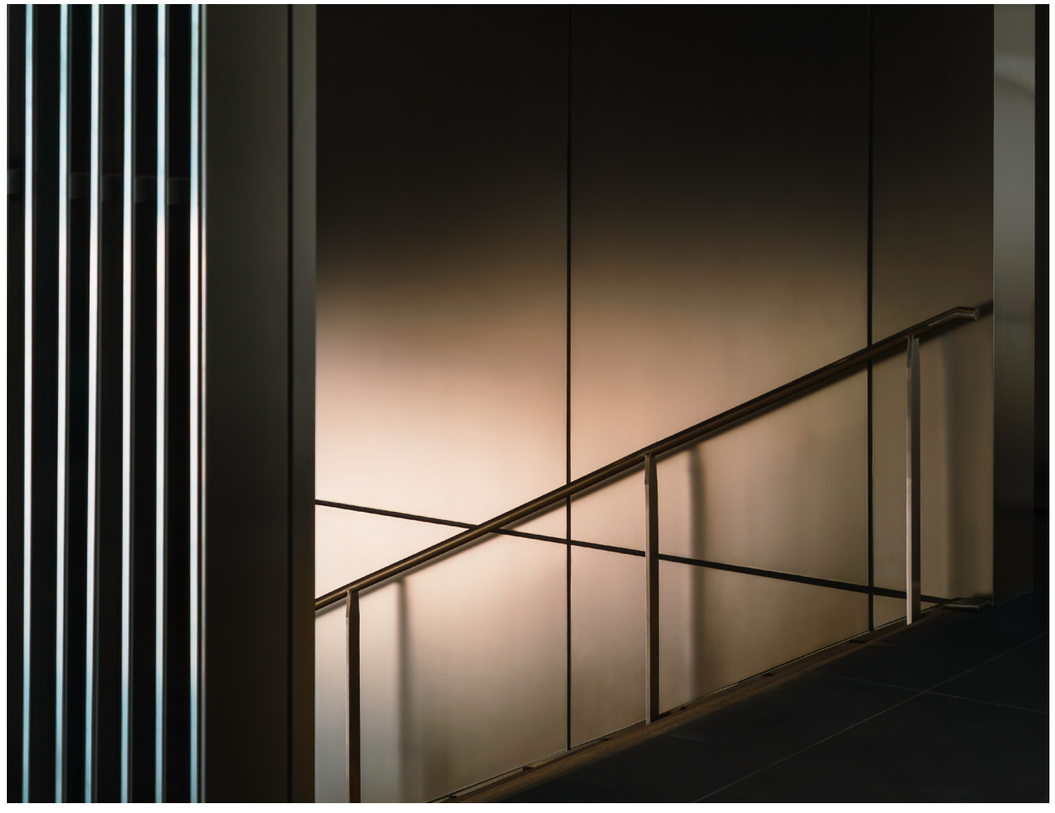


Emily Svedberg-Possfelt
COUNSEL
GÖTEBORG

[17] Guidance, paras. 197–201.
18 Guidance, section 8.3.1, 'Third-party SaaS for customer support'.
[19] Guidance, paras. 201–202(c).
[20] Draft Guidance, section 8.3.1, 'Reliance on third-party PaaS for transaction notifications'. This example does not appear in the final Guidance, although the general PaaS analysis in Guidance, para. 199, is unchanged in substance.
[21] Guidance, para. 204.
[22] Guidance, para. 207(b). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA), OJ L 333, 27.12.2022, p. 1.
[23] Guidance, para. 208.
[24] Guidance, para. 9; CRA, recital 125.
[25] Svenska Bankföreningen, Remissyttrande: Betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115), 14 April 2026, ref. 2026/01/018 (Ministry of Finance ref. Fi2026/00065), signed by Hans Lindberg and Magnus Jacobson.

The Swedish Cybersecurity Act - Where Do We Stand, and What Lies Ahead?

Nearly a year has passed since the Swedish cybersecurity act entered into force at the start of 2026. While fundamental legal provisions are now in place and supplementary regulations are being progressively implemented, some key questions are yet to be made clear - not least the interpretation of certain definitions, supervision and enforcement. This article aims to provide an overview of the act's core framework, examine where implementation and registration stands today, and looks at the challenges and developments that lie ahead.



General regarding the Swedish cybersecurity act

The Swedish Cybersecurity Act (Sw. *cybersäkerhetslagen*), hereinafter the "**CSL**", is Sweden's implementation of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (the NIS2 Directive). The NIS2 Directive (and the CSL) aims toward raising the bar for cyber resilience across the EU, ensuring organisations manage security risks, reports incidents, and that authorities have proper tools when it comes to supervision and enforcement. The CSL has been in force since the start of 2026 and is supplemented by the Swedish Cybersecurity Ordinance (Sw. *cybersäkerhetsförordningen*) and various Swedish national regulations.

As a rule of thumb, entities are in scope of the CSL if they carry out an activity in any sector covered by the NIS2 annexes[1], are established in Sweden[2], and qualify as at least a medium-sized entity - roughly meaning 50+ employees or a turnover/balance sheet above EUR 10 million. The assessment of whether an entity is in scope is made on a per-legal-entity basis.

There are some exceptions to the above-mentioned size and establishment requirements. This is for example the case for government agencies, providers of public electronic communications networks or providers of certain digital services. Entities subject equivalent sector-specific requirements, e.g. regarding security measures and incident reporting, are governed by those rules instead - notably financial entities subject to DORA (Regulation (EU) 2022/2554).[3] Notwithstanding the above, DORA-regulated entities must still register their operations with the National Cybersecurity Center under the CSL. This registration requirement applies also to credit institutions[4] that fall within the Banking sector listed in Annex 1 of the NIS2 Directive.

Core obligations for entities within scope of the CSL primarily include:

- Register with the National Cybersecurity Center (NCSC);
- Report incidents that cause or could cause essential disruptions; and
- establish and maintain a systematic approach to cybersecurity, implement appropriate security measures, and provide training for both management and staff.

<u>Something about the division of Important and essential entities</u>

Entities subject to the CSL are classified as either an important entity or as an essential entity. Generally, municipalities, regions, and entities that are larger than medium-sized enterprises[5] and fall within the sectors listed in Annex 1 of the NIS2 Directive, are classified as essential entities.[6] The remaining entities covered by the CSL are classified as important entities.

[1] The CSL covers the NIS2 Annex I "Sector of high criticality" (Energy, Transport, Banking, Financial market infrastructure, Health, Drinking water, Waste water, Digital infrastructure, ICT service management B2B, Public administration, and Space) and Annex II "Other Critical Sectors" (Postal and courier services, Waste management, Manufacture, production and distribution of chemicals, Production, processing and distribution of food, Manufacturing (various subsectors), Digital providers, and Research organisations).

[2] An entity that has a Swedish organization number is generally considered to be established in Sweden.

[3] See Chapter 1 Section 11 of the CSL. DORA is sector-specific legislation for the financial sector and takes precedence over the CSL.

[4] As defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council.

[5] See the Commission's recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC).

[6] Some entities are deemed essential regardless of size, for example government agencies and entities that are qualified providers of trusted services (Sw. *kvalificerade tillhandahållare av betrodda tjänster*). Entities identified as critical under the CER (Directive (EU) 2022/2557) will also be deemed as essential entities under the CSL.

Essential entities are subject to proactive supervision. Supervision of important entities, by contrast, is reactive and is generally triggered where there is evidence of non-compliance with the CSL. The two categories also differ in terms of sanctions. Administrative fines that may be imposed on essential entities are subject to higher caps than those applicable to important entities.[7]

Almost a year in - where do we stand, and what lies ahead?

Registration with the NCSC

Entities that fall within scope of the CSL shall register their operations with the NCSC as soon as possible. An entity that later commences an activity bringing it within the CSL's scope must file when that activity begins. Accordingly, entities that operate within any of the relevant sectors set out in the NIS2 Directive - but that do not currently meet the size threshold or other qualifying criteria - should periodically reassess their status, as changes in revenue or headcount may cause them to fall within the scope of the CSL.

Setterwalls has conducted research and consulted the relevant authorities regarding the status of the registration process, obtaining the following information. As of September 21, 2026, a total of 3297 entities has registered its operation with the NCSC. The three sectors with the highest number of registrations are: (i) Energy, with 671 registrations; (ii) Digital Infrastructure, with 654 registrations; and (iii) Health, with 598 registrations. The three sectors having the least registrations are (i) Space, with 4 registrations, (ii) Financial market infrastructure, with 7 registrations, and (iii) Manufacture of other transportation equipment (SNI C30), with 12 registrations.

It should be noted, however, that a single entity may operate across multiple sectors and may therefore have registered in more than one category. As of September 21, 2026, the aggregate sector-level registrations amount to 5073, thus exceeding total number of unique registered entities. It is also likely that there remains a certain degree of unreported cases, with further registrations expected as entities mature and become aware of the applicable requirements, whether as a result of proactive supervision, contact with the authorities, or otherwise.

Scope and some definitions remain a point of topic

Since the CSL entered into force, there has been an absence of clear guidance on a number of its key terms and definitions. The definition of cloud computing services[8] has for example prompted questions from organisations that find its scope broad and difficult to apply in practice. Although SaaS services are listed as a type of cloud computing service model potentially in scope under the NIS2 Directive[9], there is still room for interpretation whether a SaaS offering will meet all of the criteria set out for a cloud computing service under NIS2 (defined as a "*digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations*"). In particular, questions have been raised as to whether all SaaS offerings would be in scope of NIS2, including those bordering ordinary services but with application layer components hosted on hyperscalers' cloud services, or if any such offerings may be excluded from the scope. Despite recent guidelines from the Swedish Post and Telecom Authority (Sw. *Post- och telestyrelsen, PTS*) clarifying the definition of cloud computing services, these questions are yet to be fully answered.

Supplementary national regulations being progressively implemented

As regards the CSL's general requirements to implement appropriate security measures, provide training for management and staff etc., it should be noted that MSB have issued regulations and guidelines regarding (i) the registration procedures, (ii) incident reporting, and (iii) security measures (organizational, technical, and physical), including information on the content of contractual arrangements with, for example, partners within the supply chain.[10] Furthermore, the *PTS* is currently preparing supplementary sector-specific regulations on security measures for providers of public electronic communications networks, with a target of having them in place by spring 2027.

Supervision and enforcement

Each category of entity falls under the supervision of a designated supervisory authority as the allocation of supervisory responsibility is determined by the sector in which the entity operates. For example, the PTS serves as the supervisory authority for entities operating within the digital infrastructure sector. Each authority has the mandate to monitor compliance and take enforcement action within its designated area, including, for example, ensuring that entities have duly registered with the NCSC, that they have implemented security measures and established functioning procedures for the reporting of

[7] The maximum fine is: (i) *for essential entities*, the greater of 2 percent of total global annual turnover or an amount in Swedish kronor equivalent to EUR 10,000,000; and (ii) *for important entities*, the greater of 1.4 percent of total global annual turnover or an amount in Swedish kronor equivalent to EUR 7,000,000. For public entities, the maximum fine is SEK 10,000,000.

[8] A "cloud computing service" means a digital service that enables on- demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.

[9] Preamble 33: "The service models of cloud computing include, inter alia, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS)."

[10] See MCFFS 2026:1, MCFFS 2026:7, MCFFS 2026:8, and MCFFS 2026:11.

incidents.

To carry out the supervisory mandate effectively, authorities have access to a range of tools, including security scans (allowing authorities to proactively identify vulnerabilities in IT systems) and on-site and off-site inspections (enabling observation and review of an entity's operations and documentation). In addition, the authorities may conduct security audits to obtain an assessment of an entity's overall security posture. If supervision reveals that an entity is non-compliant, the supervisory authority may take enforcement actions such as issuing an order (Sw. *föreläggande*), applying for a prohibition on holding a management position (Sw. *förbud att inneha ledningsfunktion*), imposing an administrative fine (Sw. *sanktionsavgift*), or — where there are no grounds to take action against a violation in any other way — issuing a warning (Sw. *varning*).

Supervision will, according to the NSCS, be phased in gradually and will vary depending on the circumstances within each sector and the particular focus of each supervisory authority. Representatives of FRA have indicated that supervision will initially concentrate on verifying the registrations made by entities subject to the CSL, including identifying instances where such registration is absent. As the supervisory framework develops, the focus can be expected to shift from registration compliance toward more substantive assessments of whether entities have implemented adequate security measures and incident reporting procedures.

For the Banking and Financial market infrastructures sectors under the CSL, the Swedish Financial Supervisory Authority (Sw. Finansinspektionen, "FI") serves as the designated supervisory authority. FI is also responsible for supervising financial entities subject to DORA. In this capacity, FI has initiated reviews concerning cyber threats and cybersecurity in general, with a particular focus on risks arising from advanced AI models. However, the FI has so far not initiated any NIS2 specific supervision. Against this background, it is likely that FI will continue to prioritise its supervision of cybersecurity matters, potentially also including registrations under the CSL, and how entities work to strengthen their resilience.



As of summer 2026, some authorities have initiated their work with supervision and issued decisions under the CSL. The cases reviewed primarily concerned registration obligations and incident reporting, with public sector entities accounting for the majority of supervised entities. Notably, no supervisory authority has yet conducted a security audit or security scan, and no administrative fines were imposed.

Summary

Going forward, entities subject to the CSL should continue to monitor regulatory developments closely and maintain a proactive approach to compliance. The following should also be specifically considered:

- **File your notification.** Document your scoping assessment and submit the required notification to the NCSC as soon as possible. Any changes must be reported within 14 days.
- **Establish and test your incident response procedure.** The first notification is due within 24 hours, with further stages on tight deadlines. Hence, it is recommended that these incident reporting procedures are regularly tested so that routines are in place in case an incident occurs.
- **Review and prepare relevant agreements.** Cybersecurity risks must be assessed before acquiring IT systems or entering into an outsourcing arrangement. Each supplier agreement must address the relevant cybersecurity requirements under applicable guidelines and regulations. Existing agreements should also be reviewed and, where necessary, updated to ensure compliance.
- **Keep your documentation ready.** Supervisors would typically review cybersecurity compliance by requesting written documentation. Hence, up-to-date, quality-assured documentation allows organisations to respond in a more swift and accurate manner.
- **Specifically regarding the Banking sector.** Despite DORA taking precedence over the CSL, it should be specifically noted that credit institutions falling within the Banking sector listed in NIS2 Annex 1 must still register with the NCSC under the CSL.



Niklas Follin
PARTNER
STOCKHOLM



Filip Liljekvist
SENIOR ASSOCIATE
STOCKHOLM

PSD3 and the PSR: A Compliance Roadmap for Swedish PSPs

Eight years after the implementation of PSD2, Swedish and European payment service undertakings are starting to prepare for a new regulatory landscape. For the past few years, the EU has been redrawing the framework governing payment service providers. The second Payment Services Directive (PSD2) will be replaced by a directly applicable Regulation (the "PSR") and a complementary Directive ("PSD3"). At the same time, the Electronic Money Directive will be repealed and absorbed into the payment institution framework. For payment service providers and E-money institutions on the Swedish market, the implications are both far-reaching and require adaption on the part of regulated entities.

The new payment service regulations entail further harmonisation across Europe and ensure that prudential requirements apply consistently across the EU, by regulating business conduct of payment service providers directly in the PSR. However, stricter requirements set out in PSD3 will also increase the prudential and organisational requirements placed on PSPs.

Authorisation and licensing for payment and e-money institutions

Articles 44–45 of the PSD3 compromise text require existing payment institutions and electronic money institutions to demonstrate compliance with the new authorisation requirements within a transitional period. The Swedish FSA (Sw. Finansinspektionen) will need to assess each institution against the enhanced application requirements of PSD3, including the filing of a winding-up plan in case of failure, including the return of safeguarded funds in the event of a disorderly wind-up, disclosure of every application made in the preceding three years by the applicant or any group entity in any EU jurisdiction.

Whereas the originally proposed requirement for re-authorisation of payment institutions has not been maintained in the compromise texts, the requirement to provide information to supervisory authorities will force PSPs to divert time and resources to affirming compliance. Although Swedish law already requires extensive documentation for undertakings applying for authorization as a payment institution, the new regulatory regime will increase the extent of the work necessary for any potential applicants in the future.

For Swedish e-money institutions however, PSD3 will require a renewed authorisation process. PSD3 requires "a single authorisation for providers of payment services which do not take deposits", and the payment institution regime "will replace the regime applicable to electronic money institutions", extending also to non-bank issuers of e-money tokens. Electronic money becomes a payment service listed in Annex I of the PSD3, carrying its own initial capital floor of EUR 250,000 and its own own-funds method.

The general PI threshold rises from EUR 125,000 to EUR 150,000. For Swedish companies that have structured their businesses at or near the current minima, this may necessitate capital injections.



As PSD3 is a directive, Member States retain some discretion over how these authorisation requirements are implemented, for example as regards the procedure and timing of the Swedish FSA's review of existing institutions. However, the substantive requirements leave limited room for national variation, and the precise Swedish approach will only become clear once the implementing legislation is proposed.

Transaction requirements

Of the rules governing the conducting of payment service operations, the main differences compared to PSD2 relate to fraud and refunds, which will no longer be limited to unauthorised transactions, strengthening requirements on transaction monitoring and exposing payment service providers to greater liability. Transaction monitoring becomes a statutory duty on both sides of a payment, under Article 83(1a) of the PSR. The payer's PSP must monitor transactions before execution and the payee's PSP must monitor before making funds available. Where monitoring is not carried out and the payer suffers loss, the full amount is refundable, with the burden of proving compliance resting on the provider.

In particular, the PSR aims to prevent so-called spoofing fraud, where a fraudster impersonates a payment service user's PSP. Under Article 59 of the PSR, PSPs will be required to fully reimburse spoofing victims for the full transactions amount, provided the fraud is reported to the police.

Further, PSPs may no longer rely on authentication. The fact that a transaction

was authenticated, including through strong customer authentication, accurately recorded and unaffected by technical failure "shall in itself not necessarily be sufficient" to prove authorisation or user fault, and before concluding that a user acted fraudulently or with intent or gross negligence the provider must invite the user to explain the events leading up to the transaction and take that explanation into account. Further, verification of payee becomes mandatory for all credit transfers, with refund of the full amount where the service is not provided or is provided incorrectly; and consumers manipulated by a fraudster using communication channels attributed to their own provider are entitled to a full refund, subject to prompt notification and a police report, with the provider refunding or giving reasons within 15 business days and bearing the burden of proving fraud or gross negligence.

Prudential requirements and own funds

Article 6 of the PSD3 compromise text requires own funds at all times equal to the higher of initial capital and the amount produced by the applicable calculation method. The PSD2 methods survive, but a default method is introduced. Article 7(2) obliges supervisors to prescribe Method B, a sliding scale on monthly payment volume running from 4.0 per cent of the first EUR 5 million down to 0.25 per cent above EUR 250 million. Method A (ten per cent of fixed overheads) and Method C (an income indicator) may be imposed only for models executing few transactions of high individual value. Electronic money issuers shall apply Method D, two per cent of average outstanding electronic money.

The safeguarding requirements, now found in Article 9 of PSD3, are sharpened. Funds still held at the end of the business day following receipt must sit in a separate account with a credit institution or a central bank, or be invested in secure, liquid, low-risk assets. Users' funds in settlement accounts with designated payment systems now count as safeguarded provided they are not commingled, removing a cost disadvantage for institutions offering instant credit transfers. Institutions must also tell users how their funds are safeguarded, which insolvency law applies and where a claim would be raised, and concentration risk must be avoided. PSPs placing the whole client float with one bank will need to review their safeguarding.

Open banking and data access

The open banking rules move into the PSR and become materially more prescriptive.

Account servicing providers offering online payment accounts must maintain a dedicated interface (API) through which other providers can access account data or initiate payments, meeting recognised technical standards, offering performance on par with the provider's own customer interface and subject to publicly reported availability statistics.

Users must also be given a dashboard to monitor and withdraw the permissions they have granted, and providers may not create obstacles to data access, while screen scraping is banned. The practical consequence is a publicly reported service-level obligation.

Passporting and cross-border services

For PIs operating in several EU countries, passporting is streamlined. A single authorisation remains valid across the Union for both establishment and services, and Article 30 of PSD3 sets a firmer notification timetable. The compromise text also clarifies two points related to passporting. First, where an institution authorised in one Member State provides services in a second Member State via an establishment in a third Member State, the Member State to be notified is the one where the services are provided to users. Second, the requirement that an institution carry out "part" of its business in its home Member State is clarified to mean less than the majority of its business, so that home authorities may not require most of the business to be conducted there.

Consumer protection and dispute resolution

The PSR strengthens the complaints procedure for consumers. Providers must operate complaint-handling procedures in every Member State where they offer services and in the local language, and reply to all points raised within 15 business days, with a holding reply and a final answer no later than 35 business days.

Participation in alternative dispute resolution (ADR) becomes mandatory for providers, although consumers cannot be forced into it and retain their right to go to court. Member States must also allow users and consumer associations to complain directly to the competent authority. Sweden starts from a strong position,



with the National Board for Consumer Disputes already handling payment disputes, but the requirements are reinforced by harmonised administrative sanctions and daily penalty payments for ongoing breaches.

Practical implications for Swedish PSPs

For Swedish PSPs looking to adapt to the new regulatory environment, there are two main tasks ahead. The first, which concerns payment institutions and e-money institutions specifically, is regulatory mapping to ensure that the institution can show compliance with the new requirements, including the stricter own funds requirements, and preparing the winding-up plan and three-year group application history. E-money institutions will be required to undergo an extensive new authorization process, and should be prepared to produce the documentation necessary to lodge an application once the new rules enter into force.

The second, which applies to all PSPs is adapting the business to the new business conduct requirements and ensuring that the internal governance frameworks and technical solutions are adapted to comply with the strengthened transaction requirements. Framework contracts, consumer terms and outsourcing arrangements need revisiting.

The PSR applies from 21 months after entry into force, and Member States must transpose PSD3 and apply their implementing measures from the same point, when PSD2 and the Electronic Money Directive are repealed. The payee-verification provisions apply only from 27 months after entry into force, and existing payment and electronic money institutions may continue under the current framework until that same point, by which time they must have submitted the information supervisors need to assess compliance. Authorities may exceptionally extend that period by up to three months.

Whereas the payment service package has not yet been finally adopted and published in the Journal of the European Union, PSPs should already start reviewing their business and internal processes, to ensure that they are well prepared for a further harmonized and stricter regulatory environment.



Tobias Björklund
PARTNER
STOCKHOLM

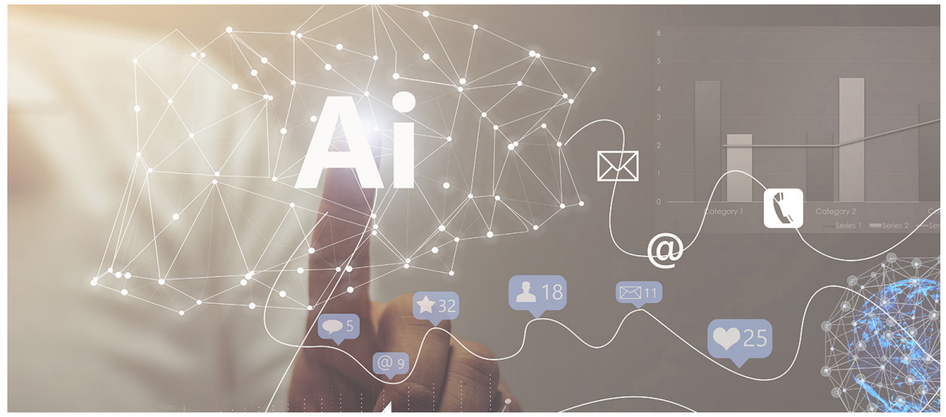


Victor Nilsson
ASSOCIATE
STOCKHOLM

Setterwalls have a strong grasp of both the legal and technical aspects of complex digital and data-driven matters, which allows them to provide clear, actionable advice.

Chambers TOP RANKED FinTech 2026 Setterwalls

Top-tier Recognition in Chambers Fintech



Feeding the AI Machine – What's Legal, What's Risky, and How do You Navigate the Grey Zones

AI is transforming the Fintech industry at speed, but building and deploying AI requires data and such data often belongs to someone else. As the industry races to stay ahead, the question of what you can lawfully collect, scrape, train on, and serve back to customers is becoming impossible to ignore. The AI Act does not provide an answer, but Copyright law does – partly. This article delves into the copyright framework governing AI training and output within the EU, with a focus on the text and data mining exception, emerging case law, and the practical grey zones that Fintech companies must navigate.

The interplay between the AI Act and existing legislation

Building and deploying AI solutions typically involves collecting and using large amounts of data, which is sometimes done by so called scraping of text, images, code, and other content from across the web. In most cases, such material is protected by copyright. Thus, when an AI model is trained or fine-tuned on such material or retrieves it through retrieval-augmented generation **("RAG")**, and then generates output that draws upon it, copyright issues arise. For Fintech companies, operating in a highly regulated environment and under increasing scrutiny, these risks need to be understood and managed.

Since the AI Act entered into force in August 2024, its provisions have gradually become applicable and it is now largely in force, but it does not regulate everything. One area that the AI Act leaves to pre-existing legislation is the intersection between AI and intellectual property rights ("**IPR**").

Copyright is to a large extent harmonised within the EU, for example by the Infosoc Directive[1], where it is stated the fundamental rights of the rightsholder to exclusively (i) authorise or prohibit reproduction of their works, in whole or in part, by any means and in any form and (ii) communicate works to the public, including making them available on demand. Both rights are directly relevant to AI systems. When an AI system scrapes content from the web, it may create copies of protected works thus engaging the reproduction right. The material is downloaded, stored, and processed to extract patterns and information from which the model learns. This amounts to reproduction regardless of whether the copies are temporary or permanent. The copyright dimension does not stop at the training phase. The same considerations apply when an entity takes a pre-trained AI model and fine-tunes it, whether for its own product development, on behalf of a customer or as part of a joint development project, or retrieves information through RAG. When an AI system produces output that incorporates or closely mirrors protected content and makes that output available to users, the communication to the public right may also come into play.

The Text and Data Mining Exception

The rightsholder's exclusive rights are not absolute. A key exception is the text and data mining ("**TDM**") exception that applies to all purposes, including commercial ones. TDM can be defined broadly as any automated analytical technique aimed at analysing text and data in digital form to generate information, patterns, trends, correlations, and more.[2] Importantly, the exception is technology-neutral and not confined to any particular method of data analysis. It applies as long as the user has lawful access to the material, for instance content freely available on the open web.[3]

Early case law has shed some light on the scope of this exception. In *Kneschke v. LAION* (Landgericht Hamburg, September 2024), a German court considered whether the TDM exception covers the scraping of images for AI training. The court concluded that creating a dataset through automated extraction and storage of images from the web fell within the TDM exception, provided that the material was lawfully accessible and no effective opt-out had been communicated by the rightsholder.

However, there is a critical grey zone. The TDM exception appears to cover the extraction and mining phase with reasonable clarity. It has, however, not yet been addressed whether the exception also extends to the output generated by an AI model. In practice, this means that a Fintech company may lawfully scrape and

[1] Articles 2 and 3 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[2] Article 4 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC ("**DSM-Directive**").
[3] Recital 18 of the DSM-Directive.

process web content for training purposes, fine-tuning or RAG purposes, yet still face copyright exposure when the AI model produces responses to end users that reproduce or closely resemble the original protected works.

***Like Company v. Google* – The Pending ECJ Ruling**

The uncertainty regarding the TDM exception is set to be addressed, at least in part, by the Court of Justice of the European Union ("**ECJ**"), in *Like Company v. Google* (Case C-411/24), where a Belgian court has referred several preliminary questions to the ECJ. One of them goes straight to the heart of the issue: does the TDM exception cover not only extraction and analysis, but also the output produced by AI systems?

Google argues that the exception should be read broadly, covering both extraction and the subsequent use of extracted information in AI-generated output. Rightsholders take the opposite view, contending that the exception was designed to facilitate analysis and research, not to provide a blanket licence for commercial exploitation of protected works through AI products.

The ECJ's ruling will matter for the Fintech industry, as the industry is data-driven and much of the relevant data is available online, but until the court delivers its judgment, the legal status of AI output derived from TDM-processed material remains a grey zone. Fintech companies should proceed on the assumption that output-side copyright risks are real and should not be dismissed simply because the input-side scraping may be covered by the TDM exception.

The Opt-Out Mechanism

Rightsholders are not without recourse. They may reserve their rights, effectively opting out of the TDM exception, by expressing such reservation in an appropriate manner. For online content, the reservation must be expressed in a machine-readable format, including through metadata and the terms and conditions of a website or service.[4]

The threshold for a valid opt-out appears to be relatively low. That said, the exact boundaries remain open to interpretation. The reservation must be adequate in both form and substance (vague or ambiguous language may not be enough, while overly broad prohibitions not specifically directed at TDM activities may also be questioned). For Fintech companies engaged in web scraping for AI development, fine-tuning or RAG, this means carefully assessing whether data sources have implemented effective opt-out mechanisms.

Grey Scales and Risk Navigation

Based on the above, the legal landscape surrounding AI and copyright is best understood as a spectrum of risk. Below we outline a practical framework showing how different scenarios carry varying degrees of legal exposure.

<u>Lower Risk</u>

- **Use of licensed material.** Content obtained under licence agreements that expressly permit both AI reproduction and publication sit on significantly firmer legal ground, providing a contractual foundation independent of the statutory TDM exception; or
- **Scraping openly available material with no opt-out.** Where content is freely accessible on the web and the rightsholder has not expressed any reservation against TDM, the extraction is likely covered by the TDM exception. The output-side risk, however, remains unresolved; and
- **Internal training use only.** Where scraped material is used solely for the internal development and improvement of AI models, without the output being made available to end users, copyright exposure is lower, as the output-side risk is not triggered.

<u>Higher Risk</u>

- **Scraping material where an opt-out is in place.** If a rightsholder has implemented an effective opt-out through e.g. machine-readable metadata, robots.txt, or terms of use, scraping such material is not covered by the TDM exception. Ignoring a valid opt-out exposes the Fintech company to infringement claims.
- **Output delivered to end users.** Where an AI model generates output that reproduces or closely mirrors protected works used in training, fine-tuning or RAG, and makes that output available to customers or the public, the risk is higher (although it should be noted that copyright protects form rather than content, and that other customary exceptions may apply). Whether the TDM exception covers such output is still an open question.
- **Scraping from sources with restrictive terms of use.** The contractual dimension should not be overlooked. Where a website's terms of use prohibit automated data extraction or restrict use for AI training, scraping in breach of those terms may give rise to contractual liability on top of copyright claims.

Conclusion

The legal framework for using copyright-protected material in AI training, fine-tuning, RAG and AI output is marked by uncertainty. The TDM exception provides a basis for extracting and analysing web content for commercial purposes, but whether it extends to AI-generated output remains, as of now, an open question.

In the meantime, Fintech companies should approach the grey zones with caution: conduct thorough due diligence on data sources, respect opt-out mechanisms and invest in licensing arrangements where possible. By staying risk-aware and monitoring legal developments closely, companies can continue to harness the power of AI while keeping copyright risks in check.

[4] See Article 4.3 and Recital 18 of the DSM Directive clarifying that rightsholders does not need to employ sophisticated technological measures.



Niklas Follin
PARTNER
STOCKHOLM



Hanna Salajin
SENIOR ASSOCIATE
STOCKHOLM



Locked In? How the EU Data Act's Cloud Switching Rights Are Reshaping FinTech Infrastructure

The European cloud market is undergoing a fundamental shift. Regulation (EU) 2023/2854 – better known as the Data Act – introduces a sweeping new framework for switching between cloud and data processing services, designed to break down vendor lock-in effects and promote genuine cloud portability across the EU. For FinTech companies, these provisions carry a double significance: not only must cloud-using FinTechs understand and prepare for the Data Act's switching rights, but many will also have to consider these new rights in light of their obligations as financial entities under the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554), which has applied since 17 January 2025.

Chapter VI of the Data Act (Articles 23-31) targets providers of "data processing services": a category broad enough to capture cloud infrastructure, platform, and Software-as-a-Service providers. The Data Act applies to any such provider, irrespective of its place of establishment, as long as it provides data processing services to customers in the EU. A FinTech company may itself be considered a provider if it supplies data processing services to others, such as to a banking client. The Act's objective is clear: customers must be able to switch to another provider, withdraw to on-premises infrastructure, or operate in a multi-cloud environment without being held back by commercial, technical, or contractual barriers.

The Data Act expressly recognises the relevance of multi-cloud approaches for digital operational resilience in the financial sector, with direct reference to DORA's own framework. For FinTechs providing cloud services to regulated financial entities, or themselves falling within DORA's scope, this intersection creates compliance requirements that deserve careful attention.

Requirements on cloud switching - and how DORA amplifies them

Under the Data Act, cloud service providers must take concrete measures to enable cloud switching. These include removing pre-commercial, commercial, technical, contractual, and organisational obstacles to such switching. Contracts must grant customers the right to switch providers, to terminate the agreement subject to a maximum notice period, and to migrate all exportable data and digital assets with reasonable provider assistance. Providers must also offer open interfaces free of charge to facilitate switching, data portability, and interoperability. For infrastructure services (IaaS) specifically, providers must take reasonable measures to ensure that customers can achieve comparable functionality (so-called functional equivalence) when migrating to another provider.

For FinTechs and financial institutions subject to DORA, the cloud switching rights under the Data Act are not merely welcome but structurally necessary. DORA requires financial entities to manage information and communication technology (ICT) risk comprehensively, including by maintaining workable exit strategies for third-party arrangements supporting critical or important functions. Article 28 of DORA requires financial entities to adopt a strategy on ICT third-party risk that includes a



multi-vendor approach where applicable, and Article 30 requires detailed key contractual provisions on service descriptions, audit rights, data access, security, and exit strategies.

In practice, the Data Act gives financial entities statutory rights they can deploy to make DORA's exit strategy requirements enforceable. Where DORA obliges the financial entity to plan for provider exits without business disruption, the Data Act obliges the cloud provider to cooperate by removing barriers, exporting data, and eliminating switching charges. The two regulations operate in parallel: DORA governs the financial entity's internal governance, outsourcing oversight, and resilience testing, while the Data Act serves as a horizontal regime that strengthens the customer's negotiation position against the provider.

Timelines and regulatory developments

The Data Act entered into force on 11 January 2024 and has applied generally since 12 September 2025. The cloud switching rights under Chapter VI therefore already apply.



However, a couple of important timing aspects lie ahead. First, the current possibility for providers to impose switching charges (although not exceeding the costs incurred by the provider that are directly linked to the switching process) will lapse after 12 January 2027. Second, providers must ensure compatibility with certain interoperability specifications and standards within 12 months after their publication. This latter requirement does not, however, apply to providers of infrastructure services (IaaS).

Separately, the European Commission has published draft non-binding Standard Contractual Clauses (SCCs) that translate Chapter VI's provisions into ready-to-use contractual terms covering switching, exit, termination, security, and business continuity during the switching process.[1]

It is also worth noting that the EU Commission's 2025 Digital Omnibus proposal suggests introducing lighter regulation in certain cases, provided the underlying contract was concluded before the general application of the Data Act on 12 September 2025. Lighter regulation is proposed for custom-made data processing services and for SMEs and SMCs providing data processing services. Notably, SMEs and SMCs would in such cases be permitted to include early-termination penalties in fixed-term contracts. This proposal remains under legislative consideration and is not yet settled law.

[1] https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding

Setterwalls FinTech Report 2026

FinTechs to-do list

- **Audit existing cloud contracts** against the Data Act's Chapter VI. Review whether your agreements include explicit switching rights, maximum notice and transition periods, data export commitments, and open interface obligations.
- **Verify cloud switching charge terms.** Confirm that any charges set out in your contracts are limited to costs directly linked to the switching process, and note the 12 January 2027 deadline for the full prohibition of switching charges.
- **Assess DORA alignment.** If you are a DORA-regulated financial entity, or act as an ICT provider to such a financial entity, map your cloud exit strategies to both DORA's Article 28 and 30 requirements and the switching rights in the Data Act's Chapter VI. Ensure the ICT third-party risk policy covers multi-vendor strategies and comprehensive exit plans.
- **Adopt the Commission's draft Standard Contractual Clauses.** Consider integrating the Commission's SCCs for cloud switching into your procurement processes, particularly for new agreements or contract renewals.
- **Watch the Digital Omnibus.** Monitor the Commission's proposal for a potential simplification of the regulatory framework.
- **Consider your timing for cloud switching.** During the transitional period, providers may charge reduced fees but remain incentivised to support the process. After 12 January 2027, switching charges will be prohibited, which will reduce costs but could potentially affect provider support.



Sophia Spala
PARTNER
STOCKHOLM



Daniel Cederquist
SENIOR ASSOCIATE
STOCKHOLM



STOCKHOLM

Sturegatan 10
101 39 Stockholm

+46 8 598 890 00
stockholm@setterwalls.se

GOTHENBURG

Sankt Eriksgatan 5
404 25 Gothenburg

+46 31 701 17 00
gothenburg@setterwalls.se