



SETTERWALLS

# FINTECH REPORT

## 2025

[setterwalls.se](https://setterwalls.se)

# Setterwalls FinTech Report 2025

## **From wait and see to momentum: the next phase for the FinTech market!?**

Over the past few years, the FinTech market has moved from excitement to caution, facing a mix of economic challenges and an expanding burdensome regulatory agenda. That caution, however, is (hopefully) giving way to renewed momentum. Klarna's IPO is a sign of a market that has reset and is now picking up pace, including more to come, within FinTech. We see deal flow, investments cooperation returning, and a more practical focus on resilience and compliance as drivers of competitive advantage.

At the centre of this next phase for the FinTech market is artificial intelligence (AI), which is accelerating product development and service delivery, while also raising regulatory and practical questions about the legal implications of developing or integrating AI solutions. Navigating complex, evolving and often cross border legal and regulatory frameworks alongside rapid technological change is a major contemporary challenge, extending well beyond the context of AI.

Much of the current framework is still relatively new, and the market has not yet developed settled practices or common interpretations. At the same time, a broader regulatory shift is under way. Efforts to simplify regulation across Europe, including the policy debate following the Draghi report, sit alongside continuing uncertainty over how rules will be interpreted and applied to FinTechs.

As a result of these observations, we have chosen to highlight some hot topic regulatory issues and trends 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 2025. We hope you find it to be both insightful and enjoyable.



*Yours sincerely,*

*Joacim Johannesson  
Partner, and Head of Setterwalls' FinTech team*

- 4**      **Sealing The Deal: Contractual Strategies When investing in IT and AI Solutions**  
Hanna Salajin & Filip Liljekvist
  
- 8**      **One year of simplification – What is the impact on European FinTech?**  
Tobias Björklund & Victor Nilsson
  
- 12**     **Back to School - From Classroom to Boardroom, a Practical Guide to Digital Operational Resilience Training under DORA**  
Emily Svedberg-Possfelt & Hugo Nerud
  
- 16**     **Demands for Accessibility in the Provision of Financial Services and Processing of Sensitive Personal Data: The Balance of Regulatory Compliance**  
Sophia Spala & Alexandra Rosell
  
- 20**     **Balancing Security and Privacy: A Guide to Background Checks for Swedish FinTechs**  
Niklas Follin & Ella von Melen

# Sealing The Deal: Contractual Strategies When investing in IT and AI Solutions

In the fast paced and highly competitive FinTech industry, the timely procurement and deployment of AI solutions can unlock substantial advantages. At the same time, investing in business-critical AI involves legal and operational commitments, alongside potentially contractual and technical risks. This necessitates a cross-functional approach involving technology, security, legal, and procurement knowledge to ensure contractual precision and adaptability with the aim of guaranteeing a sustainable AI solution throughout its lifecycle. This article provides insights and guidance on procuring critical IT infrastructure, systems, or services, focusing on various AI solutions, and how to handle associated legal and operational risks across the whole lifecycle.

## PROCUREMENT OF IT COMPRISING AI SOLUTIONS

Procuring IT solutions is a continuous process that begins well before supplier engagement. A typical procurement process when investing in critical IT infrastructure, systems, or services generally involves the following steps:

- Requirement analysis;
- Requirement setting (functional and non-functional);
- Request for Proposal (“RFP”) and bid evaluation;
- Contract drafting, negotiating and signing.

Once contracted, the IT solution may be implemented and used within the company over a long period of time. Given the extended duration from the initial requirement analysis to the decommissioning of the solution, it is important that substantial work is conducted early in the process.

The requirement analysis aims to determine, inter alia, the IT type (hardware, software, data, services), preferred delivery model, necessary resources, applicable regulatory/contractual requirements, internal resource allocation, and various risk evaluations, including weighing the IT’s business criticality, sector-specific

compliance (e.g., financial), external regulatory obligations (e.g., AI Act, GDPR), and the business’s current and anticipated future legal risk profile. The goal is to ensure that the IT solution is suitable and flexible to accommodate evolving business structures, as well as technical, legal, and regulatory changes.

## BRIEF OVERVIEW OF AI ACT-RELATED ASPECTS

The AI Act<sup>1</sup> introduces a risk-based framework impacting all companies’ developing, exporting, importing, or deploying AI. The regulation includes prohibitions for certain AI, transparency duties, and widespread obligations for specific AI categories. Key implementation milestones are staggered, with some prohibitions applying since February 2025 and August 2025, and the bulk of the framework taking effect from August 2026.

Procuring an AI solution is essentially no different from purchasing any other IT solution, but it is important to understand that the AI Act imposes different requirements depending on your company’s role within the regulatory framework and the category of AI in question. In terms of contracts, it is therefore important to define the roles of the parties, the purpose of the AI solution, data input/output (including personal data and IP-protected material), and the necessary controls for ongoing compliance. The AI Act also interacts with existing rules (e.g., GDPR and intellectual property legislation) as well as sector-specific regulations and policies, creating a complex network of compliance requirements.

<sup>1</sup> Regulation (EU) 2024/1689.

## AI CONSIDERATIONS DURING THE PROCUREMENT AND THROUGH THE IT LIFECYCLE

AI-related compliance is an evolving process requiring seamless integration between a company’s internal departments and key stakeholders. Embedding and establishing internal compliance structures should begin already in the requirement analysis phase and be an ongoing process up until the decommissioning of the solution, with the aim to mitigate and handle overall AI related risks, both internal and external towards data subjects and contracting parties.

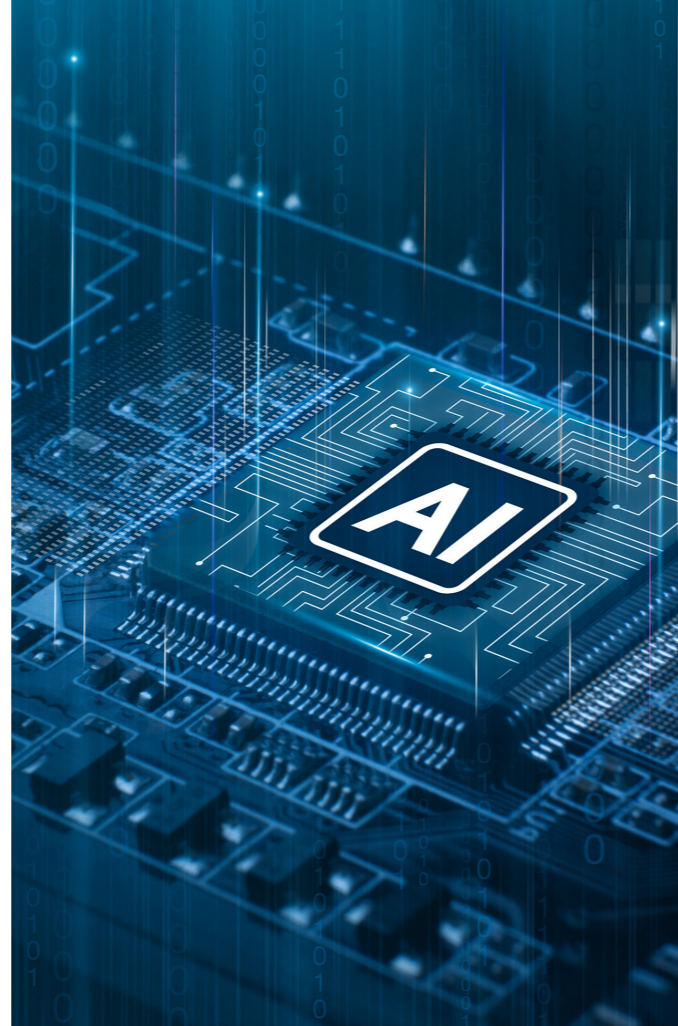
It is our general experience that the following considerations and analysis should be conducted during the respective phases of the procurement process to ensure a structured compliance process over time:

- *Requirement analysis*: Early in the procurement, a company should identify the AI solution type, its intended purpose, and its prospective regulatory role under the AI Act. This should include a thorough preliminary risk assessment, considering potential impacts on rights, safety, and data privacy, and necessary controls for continuous compliance.
- *Requirement setting (including RFP bid evaluation)*: The functional and non-functional requirements of the IT/AI solution should translate preliminary findings into concrete supplier obligations and/or contractual principles. These may encompass security standards, precise data-use parameters, and regulatory compliance, which requirements of course may be included and form part of the RFP to foster transparency, ensure a fair bid evaluation, and facilitate selecting suppliers that meets



your IT/AI-related criteria.

- **Contract drafting, negotiating and signing:** The contract should clearly and effectively translate regulatory obligations, especially for AI solutions, into clear and enforceable commitments for the contractual parties. Key provisions to be included in the contract should cover, inter alia, data ownership (including customer and training data), permissible data use (including intellectual property rights and personal data protection), and supplier restrictions (e.g., prohibiting cross-tenant training). Intellectual property rights for software, models, and other outputs should be clearly described to avoid any ambiguities, alongside customary warranties and remedies for infringement. The contract should also include, in addition to customary provisions normally included in commercial and business critical IT contracts, liability frameworks considering consequences for breaches of the AI Act, data misuse, and unauthorized training of the AI.
- **Implementation and production phase:** During the implementation and production phase, various measures should be implemented and conducted for regulatory compliance, including rolling out user training and instructions, ensuring ongoing education and policy updates, and monitoring routines and assessments. Part of this work may also include, due to the further development of the AI solution or due to changes in the company's use thereof, reassessing and evaluating the role of the company and the category of AI under the AI Act.



**BEST PRACTICE – MUST-KNOWS AND KEY TAKE AWAYS WHEN INVESTING IN IT AND AI**

In summary, investing in business-critical IT/AI may involve significant legal and operational commitments, requiring the engagement of multidisciplinary teams from the organization. The complexity of IT contracts and long duration of the IT lifecycles necessitate an adaptable solution and an underlying contractual framework that is suitable both for the current and the future business. Our market experience identifies an increase in IT contract disputes and renegotiations, driven by evolving regulations, scope ambiguities, change management issues, pricing, and contract management shortcomings. Common root causes include insufficient requirement analysis, under-resourced project governance,

and documentation gaps. To ensure a successful, timely project that addresses relevant sector needs and risks over time, we recommend considering the following when investing in material IT solutions:

- **Project based procurement:** Our experience is that material IT/AI procurements should be handled as structured projects with defined governance and steering already from the requirement analysis and up until the decommissioning. This also involves establishing leadership accountability for supplier management and regulatory engagement (e.g. cybersecurity, data protection, and AI governance).
- **Project management:** Engaging relevant stakeholders early in the project, including competences within legal, cybersecurity, technical, and general compliance is important to align system capabilities within your company's overall business and regulatory objectives. To ensure this, substantive long-term planning and assessments of market, technological, and regulatory developments are required during procurement as well during the IT lifecycle.

- **Identifying and defining the contractual and regulatory commitments:** Identifying the regulatory commitments and setting out the division of the parties' responsibilities in a transparent manner is in our view material for successful cooperation. Moreover, the contract should include, inter alia, mechanisms handling legal and technical evolution, including structured change control processes, collaboration duties, and transparent pricing adjustments.

**SUMMARY**

The use of IT solutions, especially solutions comprising AI, in the finance industry offers a compelling blend of opportunities. Financial institutions that successfully integrate this technology can reap significant rewards in terms of efficiency, customer satisfaction, and competitive advantage. However, one must also be cautious in addressing the risks and regulatory considerations that come with it. By following a structured procurement process and addressing relevant risks at an early stage, the finance industry can navigate the complexities of procuring and deploying AI solutions and savour its opportunities with minimal risks.



**Hanna Salajin**  
SENIOR ASSOCIATE  
STOCKHOLM



**Filip Liljekvist**  
SENIOR ASSOCIATE  
STOCKHOLM



# One year of simplification – What is the impact on European FinTech?

## The Draghi Report and current Omnibus Proposals

In August last year, Mario Draghi published *The future of European competitiveness*, his report on how Europe is lagging behind the US and China. The report stresses the need for reforms, noting the fragmented single market and heavy compliance load which affects SMEs (companies with fewer than 250 employees and a turnover of no more than EUR 50 million or a balance sheet of EUR 43 million) and SMCs (companies with fewer than 750 employees and a balance sheet of no more than EUR 129 million or a turnover of EUR 150 million). Many FinTechs, and in particular startups and scaleups, fall within one of these categories, and are additionally subject to financial regulations, creating an even heavier compliance load.

The report has sparked an interest in rules simplification, and the Commission elected in 2024 has made competitiveness one of its main priorities. So far, the Commission has presented seven so-called *omnibus* proposals, covering areas ranging from sustainability reporting to defense

readiness. The proposals generally aim to increase the proportionality of regulatory requirements, limiting some requirements to companies which are not SMEs or SMCs.

The Omnibus proposals have not included specific proposals related to EU financial market regulations, but nevertheless affect FinTechs, as many startups and scaleups in the FinTech sector are among the SMEs and SMCs who are affected. The major proposals impacting such FinTechs include simplified rules on sustainability reporting under CSRD<sup>1</sup> and CSDDD<sup>2</sup>, and derogations from GDPR<sup>3</sup> record-keeping obligations. The sustainability reporting requirements in Omnibus

<sup>1</sup> Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.

<sup>2</sup> Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

I would exclude SMEs and SMCs from mandatory reporting requirements, and would postpone the roll-out of CSRD requirements and CSDDD transposition. The GDPR amendments proposed in Omnibus IV exempts undertakings with fewer than 750 employees from maintaining a record of data processing activities, unless such processing is likely to result in a high risk to data subjects.

The digital omnibus package, which was published on 19 November, contains further simplification proposals, including clarifying personal data and pseudonymisation. The proposal would create a single-entry point for reporting under NIS2, DORA, eIDAS and GDPR reporting, simplifying the reporting of financial entities covered by DORA and NIS2.

The above-mentioned proposals aim to generally decrease the regulatory burden for SMEs and SMCs, and are generally not specific to FinTech companies. However, the EU's far-reaching financial regulations have also become subject to simplification. On 4 December, the Commission published a proposal on reforms to decrease and simplify regulatory requirements for financial entities and to create deeper and more integrated financial markets within the EU, increasing the amount of capital being made available to European companies and decreasing the number of European companies relocating to the US.

The proposal includes amendments to various financial regulations, including financial markets rules in MiFID<sup>4</sup> and

<sup>4</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast).

MiFIR<sup>5</sup>, the AIFMD<sup>6</sup> and UCITS<sup>7</sup> directives, and the crypto-asset regulation MiCAR<sup>8</sup>.

<sup>5</sup> Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012.

<sup>6</sup> Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

<sup>7</sup> Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast).

<sup>8</sup> Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.





Rules on trading venues are harmonised and moves from MiFID to MiFIR, increasing cross-border consistency. The financial markets regulations are further amended to increase group-level resource sharing and synergies amongst asset management groups, by specifying that such resource sharing shall not be considered outsourcing. For crypto-asset service providers, the proposed amendments to MiCAR ensure that CASPs may provide services throughout the EU without having a physical presence in a host member state. For AIFMs, ESMA is given the task of developing guidelines to ensure uniform application of prudential rules, and transmission periods between host and home member state authorities are shortened.

The proposed reforms would also centralise supervision of more financial entities – including crypto-asset service providers – to ESMA (with national licenses remaining valid during the transfer). Cross-border stock exchanges, clearinghouses and central securities depositories would also be supervised by the Paris-based agency.

**Conclusions**


The existing omnibus proposals and financial market rules reforms would be expected to decrease the compliance load for European and Swedish FinTechs, especially those who are SMEs or SMCs. Those entities would be able to focus more on product and upscaling, and less on complying with various EU regulations.

However, there are still many obstacles to rules simplification in practice. The existing omnibus proposals are subject to debate both in the European Parliament and among member states,


with more than 1,000 amendments proposed just to the Omnibus I proposal in Parliament, and the risk of national ‘gold-plating’ creating a non-uniform regulatory environment remains.

It is far from certain what the final amendments to EU regulations will look like. Yet, if the proposals were to enter into force in their current form, small and medium-sized FinTechs would not only be able to redirect resources from compliance to product

development, but a lower regulatory burden and centralized supervision could potentially also favour expansion into other European jurisdictions for some FinTechs. The current simplification proposals are also likely not the endpoint of EU regulations but could signal a fundamental shift towards proportionality and decreased compliance loads for European companies.



**Tobias Björklund**  
PARTNER  
STOCKHOLM



**Victor Nilsson**  
ASSOCIATE  
STOCKHOLM



# Back to School - From Classroom to Boardroom, a Practical Guide to Digital Operational Resilience Training under DORA

## Introduction

*As part of the EU’s Digital Decade strategy, the EU adopted the Digital Operational Resilience Act (“DORA”) on the 17<sup>th</sup> of January 2025. DORA aims to strengthen cybersecurity within the financial sector and turned “digital resilience” from a boardroom buzzword, into everyday practice for financial entities within the EU.*

*The need for DORA is rooted in the rapid digitalization of our society and the growing number risks and threats connected to the use of Information and Communication Technology (“ICT”). DORA aims to combat these threats and risks with inter alia mandatory hands-on operational resilience training. As such, it is time for all staff, management, and, where appropriate, ICT third-party service providers of DORA-entities to go back to (cybersecurity-)school and learn a thing or two about operational resilience.*

*If you are a DORA entity struggling to*

*understand what this all means, this article is for you.*

## No One-Size fits all

DORA Article 13(6) requires financial entities to embed digital operational resilience training as compulsory modules (no opt-outs) within staff training programmes across all levels of the organisation. The content should be tailored to the role and responsibilities of each audience. While certain core topics will be relevant to everyone with access to ICT systems, the depth and specificity of training must reflect the functions and risk exposure of different staff groups—**because jobs differ and so should training.**

In practice, personnel with elevated privileges—such as IT administrators and senior management with privileged system access—should receive more advanced instruction, for example on the fun (and sensitive) stuff:

secure authentication mechanisms and privileged access management. By contrast, staff with limited data access should receive foundational training that covers password hygiene, multi-factor authentication, phishing awareness, and general security practices—the basics we all know and occasionally forget. The objective is to align training intensity with potential impact on the organisation’s ICT environment.

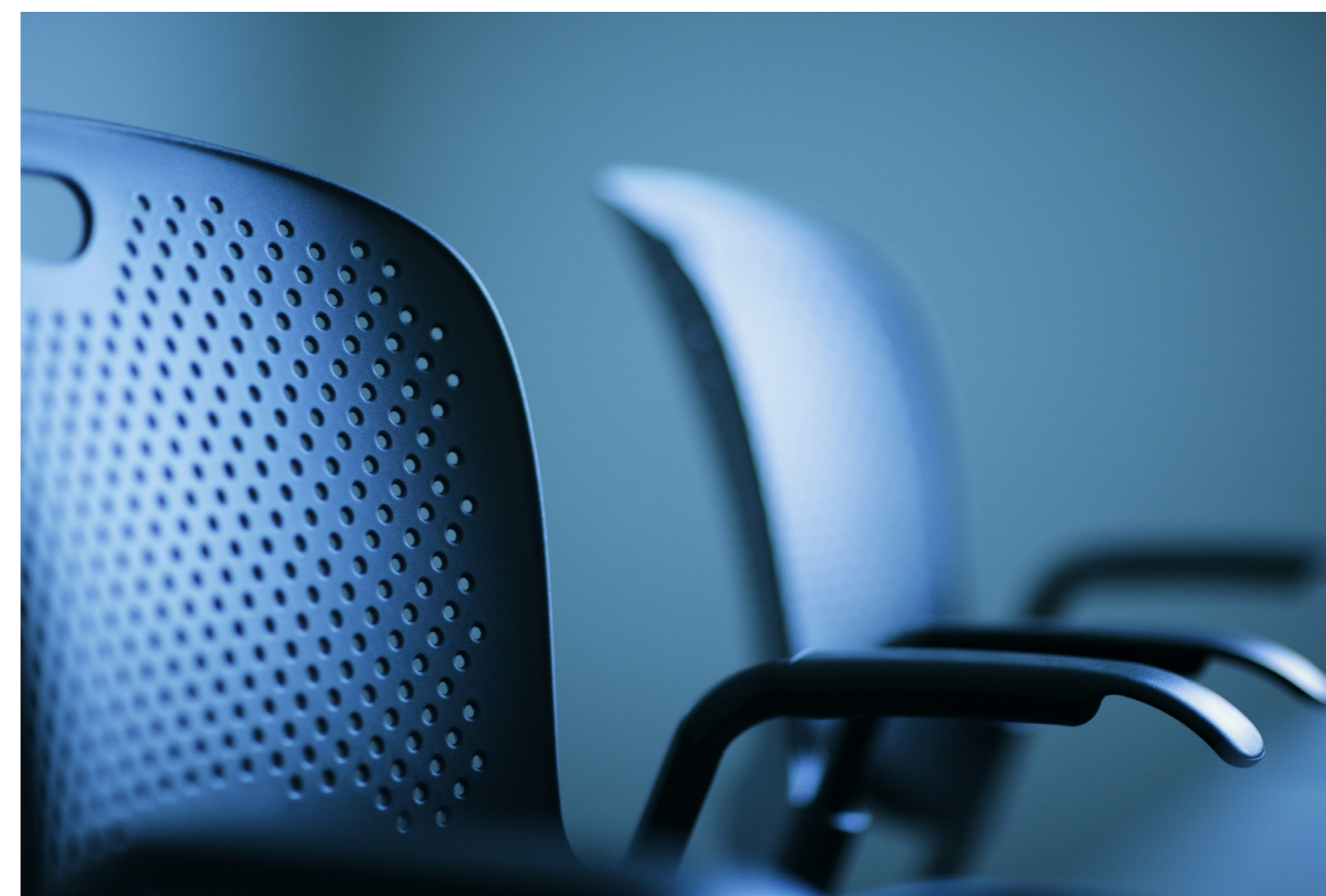
Training must also be proportionate and risk-based—no need for heroics for low-risk, no half-measures for high-risk. Entities facing higher inherent or residual risk are expected to design and deliver more sophisticated and frequent training, whereas entities with lower exposure may reasonably implement a lighter programme. Traceability is critical: document the rationale, design decisions, delivery,

attendance, assessment results, and continuous improvement measures to demonstrate how the training architecture aligns with your entity’s risk profile and evolving threat landscape. **If it isn’t documented, it didn’t happen.**

There is no one-size-fits-all training blueprint—and that’s a feature, not a bug. Each entity should calibrate its curriculum to its organisational structure, technology stack, risk appetite, and regulatory obligations. The following steps is one way to operationalise this in practice, accompanied by practical considerations to support implementation and ongoing compliance. Your mileage may vary.

## **Step One - Who’s on the hook? Map your people before you train them**

Once you’ve acknowledged your status as a DORA-regulated entity with a duty to implement training, start by charting the



landscape of your staff and ICT third-party service providers across your organisation.

The goal is simple: **identify exactly who must be in scope for training.** In a compact organisation, this may be refreshingly straightforward. In a sprawling group with multiple business lines and a thicket of outsourcing arrangements, it can be more of a treasure hunt—so be systematic, thorough, and a little ruthless about who needs to be included.

**Step Two – Map your people to your cyber risks**

In step two, line up your mapped staff populations against the ICT risks you’ve actually identified—no guesswork, just evidence.

Start with the obvious cross-cutting scenarios: credential theft, phishing, and business email compromise. If someone has an email account tied to internal systems, they’re a phishing target. If they’ve got remote access or privileged rights, they’re a higher-risk target. And if they help run a critical or important function, they need scenario-based training that tracks to continuity and recovery expectations—because when things wobble, they’ll be holding the steering wheel.

Keep it simple at first. **Set a baseline curriculum for everyone** that covers cyber hygiene fundamentals, secure data handling, and internal reporting and comms protocols. **Then layer** on role-specific modules for the higher-risk cohorts—privileged users, remote workers, and operators of critical processes. The result is training that’s right-sized, risk-aligned, and frankly more effective than death-by-slides.

**Step Three – Train your ICT third-party service provider, and perhaps re-write the fine print**

Where it makes sense, bring your ICT third-party service provider into the school room—and make sure your contracts say that they will have to show-up and take notes.

In line with step two, map ICT risk to each ICT third-party service provider by zeroing in on services that underpin critical or important functions, involve privileged access, or are delivered on-premises. If the current agreements don’t oblige ICT third-party service provider to receive the right training for the risks they introduce, then it’s time to sharpen your pencil and renegotiate. Better training, better resilience, fewer surprises.

**Step Four – It doesn’t have to be boring**

DORA doesn’t prescribe the format or delivery of training, which is both a blessing and a trap. You can stick to slide decks if you must, but relying solely on PowerPoint is a quick way to lose the room. A smarter approach and a better success (from what we have seen from our work with clients) is to treat the slides as the spine—not the whole body—and layer in activities that get people thinking, clicking, and actually doing.

Start with short, sharp decks to set the scene and reinforce the “why,” then blend in practical, real-world exercises that mirror your risk profile and operating model. Aim for sessions that feel like they matter on Monday morning, not just on compliance reporting day. For example, you might weave in the following to bring

the material to life and build muscle memory across the business and the management body:

- Phishing simulations delivered via email campaigns that escalate in sophistication over time, with tailored feedback for individuals and teams.
- Hands-on incident response exercises aligned to your established playbooks, so the incident response team practices roles, decision points, and communications under time pressure.
- Structured walkthroughs of ICT response and recovery plans that surface dependencies, RTO/RPO assumptions, and who does what when the lights flicker.
- Mandatory knowledge checks for management bodies focusing squarely on governance duties, escalation thresholds, and accountability under DORA.

The result is a programme that doesn’t just tick the regulatory box—it strengthens operational resilience, sharpens decision-making, and nudges behaviours in the right direction. If attendees leave with a few hard lessons, a couple of good questions, and a clear sense of ownership, you’ve done it right.

**Step Five – Close the loop**

Now it is time to close the loop. Document your training programme comprehensively and define clear indicators to measure its effectiveness. Integrate lessons learned from actual incidents and insights from testing into the curriculum to ensure continuous improvement. By regularly updating and evolving the training, you will remain aligned with the latest cybersecurity practices.

DORA compliance is not a one-off exercise: training must be delivered on a recurring basis to keep knowledge current and capabilities sharp at all times.

**Ending Comment**

An effective training programme is proportionate, risk-based, role-specific, and continuously refined in response to incidents, testing outcomes, and technological change.

By mapping people to the risks they face, developing engaging, relevant content, and incorporating ICT third-party service provider where appropriate, you lay the groundwork for a robust, bespoke training framework. Done well, this approach drives meaningful behavioural change where it matters most.



**Emily Svedberg-Possfelt**  
COUNSEL  
GÖTEBORG



**Hugo Nerud**  
ASSOCIATE  
GÖTEBORG



# Demands for Accessibility in the Provision of Financial Services and Processing of Sensitive Personal Data: The Balance of Regulatory Compliance

The internal market is a cornerstone of European collaboration, ensuring the free movement of goods, services, capital, and people. However, to make these freedoms accessible to all, certain actions are required by service providers and the EU has taken significant steps to ensure such accessibility. This article examines the EU's new legislative act on accessibility, particularly in light of the potential processing of personal data required to comply with the legislation.

## 1. The legal landscape

In recent years, businesses of all sizes have faced an increasingly complex array of harmonized legal requirements, presented in different kinds of legal documents, that must be integrated into their daily operations. These requirements all necessitate

compliance efforts, financial commitments, and competency enhancement measures for employees at all levels.

The financial sector has long been a focal point of regulatory compliance, and this trend shows no signs of abating.

## 2. The European Accessibility Act and the Swedish Implementary Act

The European Accessibility Act (the 'Act')<sup>1</sup> is a directive aimed at improving the functioning of the internal market for accessible products and services by removing barriers created by divergent national legislation. Through these efforts, the Act seeks to eliminate

<sup>1</sup> Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

and prevent any obstacles to free movement.<sup>2</sup>

Consequently, the directive establishes common rules on accessibility within the EU to facilitate cross-border trade and expand the market for accessible products and services.

During the preparation of the Act, the most important products and services for people with disabilities were identified, including banking and financial services aimed at consumers, both physically and digitally provided.

According to the preparatory works of the Act, specific accessibility requirements apply to all products and services covered by the Act, provided that these do not alter

<sup>2</sup> See [Accessibility of products and services | EUR-Lex](#).

the basic nature of such products and services, or impose a disproportionate burden on the operators. For products, the requirements include designing and producing them to maximize their use by people with disabilities, as well as complying with detailed rules on information and instructions, user interface and functionality design, support services, and packaging. For services, the equivalent requirements include providing information about the service, its accessibility features and facilities, making websites and mobile devices easily accessible, and applying practices, policies, and procedures to address the needs of people with disabilities, with specific rules applicable to different services.

Service providers, such as those offering banking and financial services, must design and provide their services in accordance with the Act. They must make available to the public both written and oral information that is easily accessible to people with disabilities, regarding the services they offer and how the accessibility requirements are met. Additionally, they must ensure that procedures are in place to continue conforming with the accessibility requirements and to account for any changes.<sup>3</sup>

As of 28 June 2025, the Swedish legislative act incorporating the Act entered into force, known as the Swedish Accessibility Act (the 'Swedish Accessibility Act')<sup>4</sup>. This legislative act enumerates the banking and financial services covered by the Act as follows:

- credit agreements covered by the Consumer Credit Act (2010:1846),
- the services referred to in Chapter 2, Section 1, items 1, 2, 4 and 5, and Section 2, items 1, 2, 4 and 5 of the

<sup>3</sup> [European accessibility act - European Commission](#)

<sup>4</sup> Sw. Lag (2023:254) om vissa produkters och tjänsters tillgänglighet.



- Securities Markets Act (2007:528),
- payment services as defined in Chapter 1, Section 2 of the Payment Services Act (2010:751),
- services related to the opening, use and closing of a payment account, including payment services and payment transactions covered by Chapter 1, Section 7, item 1 of the Payment Services Act, as well as overdraft facilities and services that permit the balance on a bank account to be exceeded,
- electronic money as defined in Chapter 1, Section 2, item 2 of the Electronic Money Act (2011:755), and
- payment terminals as defined to enable the execution of payments using payment instruments as referred to in Chapter 1, Section 4 of the Payment Services Act (2010:751) at a physical point of sale, but not in a virtual environment.

### 3. Processing of personal data

In Sweden, the primary legal frameworks relevant for the processing of personal data are the General Data Protection Regulation (“GDPR”)<sup>5</sup> and the Swedish Data Protection Act<sup>6</sup>. The latter complements the GDPR by introducing specific Swedish provisions necessary for its interpretation, such as those relating to freedom of expression and within the field of employment.

Under these frameworks, *personal data* is defined as any information that can directly or indirectly identify a natural person. In addition, certain types of personal data are classified

<sup>5</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>6</sup> Sw. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

as particularly sensitive – referred to as *special categories of personal data* under the GDPR. This category includes information that may reveal, for example, an individual’s health status, sexual orientation, or religious beliefs.

The GDPR presents requirements for anyone *processing* personal data to clearly, and in a manner suitable for the individual who’s personal data is being processed (the “**data subject**”), inform of their processing activities. This information must include details about said processing activities, such as the purpose, legal basis, and any third parties with whom the personal data is shared.

When considering this legal framework in relation to the obligations under the Act, it becomes evident that there are areas where the requirements overlap and interact.

### 4. Calculating compliance – accessibility and processing of personal data

When implementing the Act and the Swedish Accessibility Act within an organisation, while also considering the potential processing of personal data, it is essential to assess the meaning of accessibility in the financial sector. For example, online banking services must be accessible to all users, which requires, among other things, clear and precise information, intuitive navigation, user-friendly interfaces, and adaptable design.

Furthermore, in the context of the financial sector, measures to ensure accessibility in physical environments may include, for example, ramps to facilitate access to ATMs, clear directional signage, and the availability of various hearing aids in meeting rooms for consumers. For digital

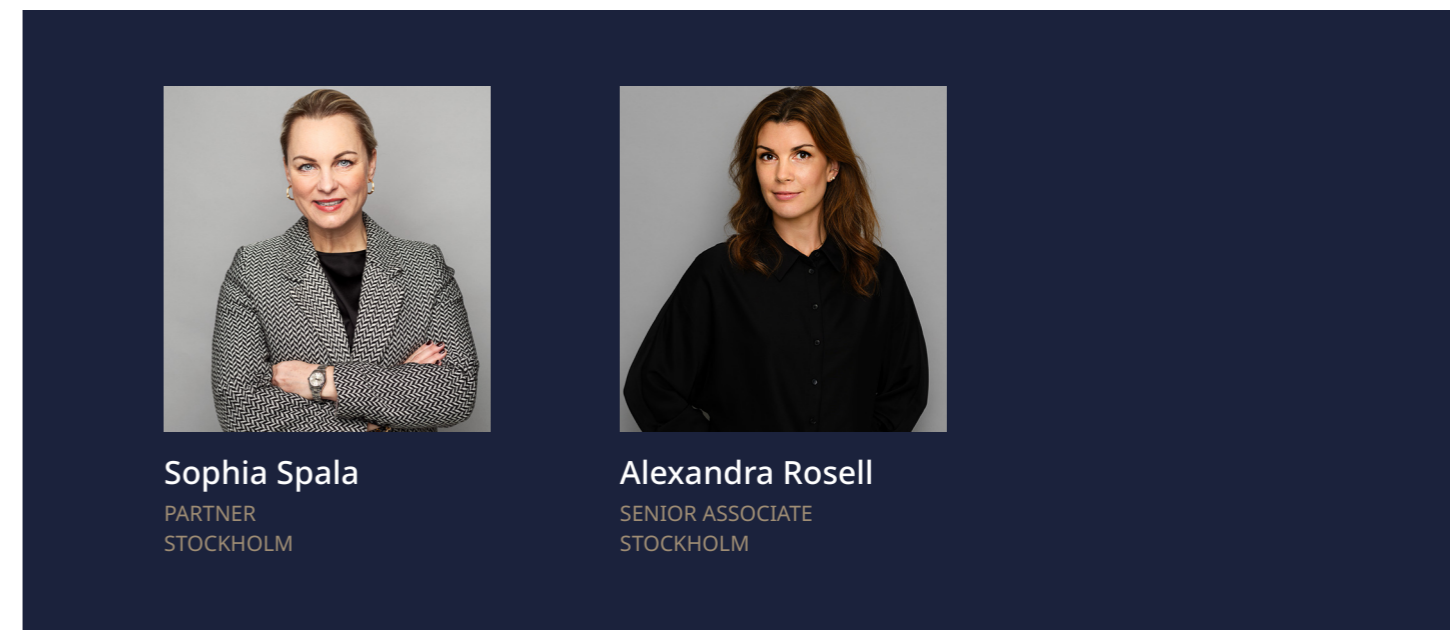
environments, measures such as ensuring sufficient contrast between text and background and providing audiovisual aids to facilitate access to information should also be considered.

As with many compliance-driven initiatives, considerable effort is devoted to ensuring adequate documentation and providing relevant information to affected parties. However, in addition to implementing policies describing accessibility measures and internal procedures, financial institutions must also assess and ensure compliance throughout their entire supply chain. For example, while primary efforts may focus on marketing and publicly available resources, it is important not to overlook the need for compliance for consumers who are logged in (such as for messaging, internet banking, or making payments).

When considering and implementing these accessibility measures, it is not unlikely that they will involve processing of personal data. For instance, when offering different options in the user interface, consumer preferences will

become visible to the service offering financial institution, resulting in the institution processing personal data of the consumer. This is since a consumer’s selection of bold text or hearing aids in its use of the financial institution’s services may, strictly speaking, constitute processing of personal data relating to health, which is classified as a special category of personal data under the GDPR. Consequently, compliance with the Act will also necessitate compliance with the GDPR.

In line with the above, we recommend providers of financial services to take the GDPR into consideration when undertaking compliance projects aimed at improving the accessibility of their services. Where appropriate, they should also prepare or update necessary risk assessments, including impact assessments where relevant, as well as general GDPR documentation, such as privacy policies, data processing agreements, and records of processing activities.



**Sophia Spala**  
PARTNER  
STOCKHOLM



**Alexandra Rosell**  
SENIOR ASSOCIATE  
STOCKHOLM



# Balancing Security and Privacy: A Guide to Background Checks for Swedish FinTechs

Companies, and especially FinTechs, are under increasing pressure to know their personnel as well as they know their customers. From sanctions compliance and AML/KYC to access controls and fraud prevention, background checks and security vetting are often indispensable. Yet Swedish law offers no single definition of “background check,” and the legal framework is fragmented. As a result, many organisations find themselves operating in a grey zone, balancing legitimate security needs against stringent data protection rules.

## Navigating Background Checks in Sweden: A Legal Grey Zone

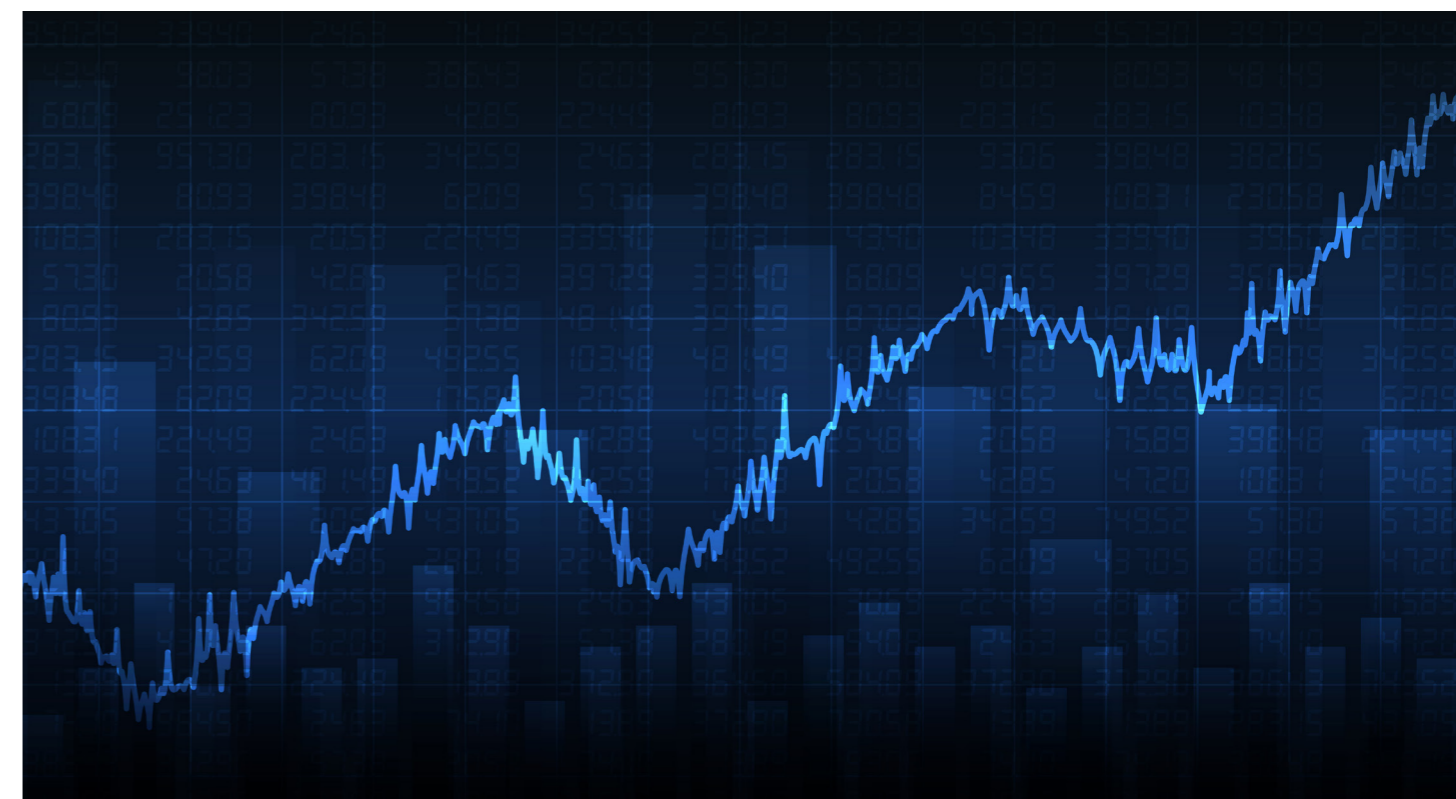
Companies, especially those under the supervision of the Swedish Financial Supervisory Authority—subject to, *inter alia*, requirements under AML and DORA<sup>1</sup>—must proactively identify and manage risks, including those related to their personnel. Background checks (Sw. Bakgrundskontroller) are therefore a key tool for verifying information and uncovering potential risks regarding employees, individual consultants and candidates during recruitment. However, these checks must always be proportionate and carefully balanced against the individual’s right to privacy.

Conducting background checks means navigating a complex legal landscape, with the GDPR<sup>2</sup> always at the forefront since personal data is almost always involved. Yet, Swedish law offers no clear definition or explicit prohibition on background checks, leaving employers in a legal grey zone. The term “background check” therefore covers everything from simple reference checks to sensitive reviews of credit history, tax records, sanctions lists, and (most sensitive of all) criminal records. The absence of clear rules highlights the urgent need for guidance and a unified legal framework.

This article navigates you through the legal maze surrounding three

<sup>1</sup> Regulation on digital operational resilience for the financial sector (EU) 2022/2554.

<sup>2</sup> General Data Protection Regulation (EU) 2016/679.



particularly sensitive areas of background screening—criminal records, sanction lists, and financial information—and offers practical guidance for conducting checks in a compliant and proportionate manner. We also share best practices—advise and round off with a look ahead at the legislative changes that are set to reshape the landscape.

## Criminal Records: When Are They Really Allowed?

As a rule, private actors are generally prohibited from processing personal data related to criminal convictions and offences. Under GDPR and Swedish supplementary law,<sup>3</sup> such processing is only permissible when necessary to establish, exercise, or defend legal claims, or to fulfil specific statutory

<sup>3</sup> Article 10 GDPR and section 5 Swedish regulation (2018:219) with Supplementary Provisions to the GDPR.

or regulatory obligations. Swedish law provides such authorizations narrowly, primarily for certain financial sector activities and other regulated areas. Further, the Swedish Authority for Privacy Protection (IMY) has issued general permissions for a handful of narrowly defined contexts,<sup>4</sup> and it may grant exemptions on a case-by-case basis upon application. In practice, most employers do not have, but typically, employers lack a general right to process criminal record data.

Two limited avenues exist to obtain criminal record information without direct employer processing: an organisation may ask an individual to bring and display a criminal record extract during a physical

<sup>4</sup> Such as entities under the supervision of the Swedish Financial Supervisory Authority, as well as within the social services sector and the education sector according to section 6 of IMY’s provisions on the Processing of Personal Data Related to Criminal Offenses (IMYFS 2024:1).

meeting, without the organisation making any copy or note of its contents beyond recording that the extract was presented,<sup>5</sup> or a specialist provider holding separate right such as an IMY permit for handling criminal records data can conduct the screening; in such case the provider's permit conditions will govern the process, and results are typically delivered orally and in summary form.

In all other scenarios, companies may have issues finding sufficient legal basis and should in such case refrain from requesting, collecting, or recording information about criminal offences. Where criminal record checks are permissible, proportionality is crucial: restrict use to roles with genuine risk exposure, avoid retaining results, and document only the fact of presentation and the decision made.

**Sanctions Screening: Essential, Yet Heavily Regulated**

The expansion of EU and UN measures in recent years has significantly increased the importance of sanctions screening. For financial institutions regulated by the Swedish Financial Supervisory Authority and actors in security and defence markets under the Inspectorate of Strategic Products, processing criminal offense data for sanctions checks may be permissible to the extent necessary to comply with regulatory requirements. IMY's general authorization<sup>6</sup> permits such entities to process criminal offense data for screening personnel and candidates against official sanctions lists, including those of the EU and UN.

Under this authorization, companies conduct screenings directly against

<sup>5</sup> Adverse findings must be handled verbally.  
<sup>6</sup> Section 6 of IMY's provisions on the Processing of Personal Data Related to Criminal Offenses (IMYFS 2024:1).

official lists or use reputable third-party vendors. As always, organisations must ensure a valid GDPR legal basis, strict purpose limitation, and minimise necessary data retention for auditability. For companies outside IMY's general authorization scope, sanctions screening of staff or candidates may still be justifiable but necessitates careful analysis to avoid unlawful processing of offense-related data.

**Financial Background Checks: Striking the Right Balance**

Financial data, such as income levels, tax information, credit histories, property holdings, debt, or payment defaults, while not per se categorized as 'special category' data under article 9 GDPR, presents heightened privacy risks and may require additional justification. Swedish guidance indicate that some collection of income information may be permissible based on legitimate interests, provided a documented balancing test clearly demonstrates the employer's need outweighs individual privacy. By contrast, collecting broader financial information (e.g., property holdings or debt) generally demands stronger justification, often limited to roles with extensive decision-making authority and significant financial responsibility.

Credit checks are subject to specific regulations, requiring a legitimate need (e.g., an existing or impending credit relationship or a justified financial risk assessment). For employers, this could restrict credit checks to roles where financial integrity is a bona fide requirement, and less intrusive measures are insufficient. In all cases, companies must define scope, avoid bulk collection, ensure transparent privacy notices, and implement short

retention periods.

**Best Practice Blueprint: Structure, Transparency, and Control**

In this grey area, structure is your best friend. Communicate clearly with employees and candidates about if, when and how background checks are performed. If you use external screening providers, make sure to align on roles and responsibilities under the GDPR, put appropriate contracts in place, and agree in advance how results will be reported. And lastly, adopt a written policy that defines your organisation's routines for a "background check," the trigger points and timing, the roles it applies to, the legal basis, and the documentation and retention framework. Keep the scope proportionate and be prepared to justify your approach.

**On the Horizon: Legal Reforms and What to Do Now**

Change is coming. IMY has called for greater legal clarity and an inquiry into background checks which has resulted

in the Swedish government initiating a review into background checks, which is to be reported no later than 11 March 2027.<sup>7</sup> There are also pending law-reform initiatives addressing expanded register controls in specific public-sector settings,<sup>8</sup> as well as recent Supreme Court rulings interpreting GDPR-related constraints on processing offence-related data.<sup>9</sup>

Until a coherent and a sufficient sector-agnostic framework is adopted, companies should continue to apply the current rules wisely. Clarity in process now will position you well when the law catches up.

<sup>7</sup> Committee Directive – An Appropriate Regulatory Framework for Background Checks (Dir. 2025:83).  
<sup>8</sup> Referral of the Council of Legislation – Expanded Register Checks for Employment in Municipalities, 9th October 2025.  
<sup>9</sup> NJA 2025 s. 123 "GDPR and Criminal Judgments I and II".



**Niklas Follin**  
 PARTNER  
 STOCKHOLM



**Ella von Melen**  
 ASSOCIATE  
 STOCKHOLM





STOCKHOLM

Sturegatan 10  
101 39 Stockholm

+46 8 598 890 00  
[stockholm@setterwalls.se](mailto:stockholm@setterwalls.se)

GOTHENBURG

Sankt Eriksgatan 5  
404 25 Gothenburg

+46 31 701 17 00  
[gothenburg@setterwalls.se](mailto:gothenburg@setterwalls.se)

MALMO

Stortorget 23  
203 20 Malmoe

+46 10 690 04 00  
[malmoe@setterwalls.se](mailto:malmoe@setterwalls.se)