AC Audio: Fintech and New Regulation

[00:00:07.530] - Ian Duffy, Partner

Hello and welcome to this Arthur Cox podcast. Over the last number of years, regulated firms have had to get to grips with a wave of new laws and regulations around data protection, outsourcing, operational resilience and information security and there's plenty more on the horizon in terms of new rules around artificial intelligence. So understandably, most of the focus in looking at these rules has been on the regulated firms that they actually apply to but what about the technology service providers to these firms? Today, Ciara Anderson and myself are going to discuss some of the recent and emerging laws in this space and how they are relevant to Fintech providers. As part of this, we'll look at the Digital Operational Resilience Act, DORA, the revised Network and Information Systems Directive, NIS 2, and the soon to be finalised Artificial Intelligence Act but before we get into that nitty gritty, let me introduce myself. My name is Ian Duffy, Partner in the Technology and Innovation Group here at Arthur Cox, and I lead our Outsourcing and Digital Transformation Practice and as I mentioned, I'm joined by my colleague Ciara.

[00:01:08.350] - Ciara Anderson, Senior Associate

Hello everyone. My name is Ciara Anderson. I'm a senior associate on the Tech and Innovation Team here at Arthur Cox, and I work closely with Ian on digital transformation and outsourcing projects.

[00:01:19.130] - Ian Duffy, Partner

Okay, thanks Ciara. So then, diving into some of the specifics, I think a good starting point for us here is to set out some of the regulatory obligations that currently apply to Fintech providers and our first key stop is around data protection. So Fintech providers who process personal data must comply with relevant requirements of the GDPR and relevant domestic implementing legislation. So in Ireland, that's going to be the Data Protection Act 2018. Many Fintech providers will likely act as a processor under the GDPR when they're processing personal data as part of the services they provide. However, there might be some circumstances where Fintech providers will use their customers data for their own purposes and are likely to act as a controller. So a good example of this is where a fintech provider might use some of its customer data to improve its products. So in terms of compliance with specific standards in their role as processors, one of the key areas is that Fintechs will need to implement appropriate security measures, and one way in which they can help to achieve this is through looking to align with industry standards, so the likes of ISO 27,001 and ISO 27,002.

[00:02:28.430] - Ian Duffy, Partner

Additionally, more practical measures such as implementing robust information security policies and conducting tabletop exercises can also be very helpful when it comes to aligning with GDPR information security standards. Fintech providers also need to be mindful to ensure that their contracts with their customers include appropriate processor provisions to help their customers align with the requirements of Article 28 of the GDPR. It's also worth mentioning and reiterating that appropriate security measures is

something that fintech providers will also have to be very mindful of where they're acting as a controller and another important point for fintech providers when they're acting as a controller will be the GDPR's transparency requirements. So this is effectively informing data subjects of how and why you use their personal data and compliance with transparency requirements can be achieved through ensuring that data subjects receive an appropriate data protection notice, whether you communicate that yourself or your customers communicate that data protection notice on your behalf. So, Ciara, I might hand over to you to now discuss existing obligations under the NIS directive and the incoming NIS 2 Directive.

[00:03:41.420] - Ciara Anderson, Senior Associate

Sure, Ian. So it's important to note that some, but not all, Fintech providers will be subject to the NIS Directive, which was transposed in Ireland back in 2018. So the NIS directive really was the first EU wide cybersecurity law that is not specific to personal data like the GDPR, and it's focused on ensuring that entities covered by the Directive will apply a specific minimum cybersecurity standard, and it also contains certain reporting obligations for significant cybersecurity incidents. So the NIS Directive, as Ian mentioned, is due to be replaced by NIS 2, which is an evolution of the requirements of the NIS Directive, rather than a drastic overhaul of the cybersecurity requirements in the EU. So under NIS 2, the scope of the application we saw in the first NIS Directive is going to be expanded. So it's going to include ICT managed service providers that implement software and ICD managed security service providers. So they will be covered under the scope of the new NIS 2 Directive. So the first thing will be for Fintech providers to determine if they're within this broader scope of NIS 2. If so, they should look to align their existing incident response and cybersecurity management framework to meet these new requirements.

[00:04:59.190] - Ciara Anderson, Senior Associate

And one of the more important things to highlight about NIS 2 is the shorter incident notification timeline. So it's gone from 72 hours reduced down to 24 hours for notifications of significant ICT incidents. So Fintech providers will need to review and ensure that their own internal incident management processes align with this new shortened timeline. There are other prescriptive obligations under NIS two that may apply, such as requirements to have in place encryption, for example, or multifactor authentication. It touches on supply chain security, and then there's other prescribed technical measures as well. In terms of timing, the NIS 2 Directive is currently in force, but because it's a directive, it has to be transposed, and member states have until 18 October 2024 to do that. So there is some time for Fintech providers to take stock, determine if they're within scope, and prepare for compliance. So so far, Ian's covered data protection obligations, we've covered cybersecurity obligations, and another important consideration for fintech providers will be whether their arrangements with their regulated customers will be subject to applicable outsourcing rules. So Ian, do you want to touch on what those rules are?

[00:06:13.050] - Ian Duffy, Partner

Yeah, absolutely, Ciara. So I think from an Irish perspective, the key set of outsourcing rules will be the CBI's cross industry guidance on outsourcing, and they generally apply to all regulated firms in Ireland,

and in particular for the purpose of looking at them in the context of Fintech providers. I'll focus on certain requirements under that guidance which prescribe that certain contractual provisions have to be included in the contract between a regulated firm and its service provider, which for our purposes here, could be a Fintech provider. So, like I said, the guidance is applicable to all regulated firms in Ireland, and it's really focused on ensuring that regulated firms effectively manage and mitigate the risks associated with outsourcing of critical services. So for Fintech providers in Ireland who contract with regulated firms, the contract will need to include certain provisions, like I mentioned, and these provisions are very much focused on ensuring that regulated firms have reasonably broad rights and remedies designed to assist them with managing their relationship with the provider, and also mitigating some of the risks associated with outsourcing so the types of areas that these contractual provisions cover include areas like access and audit rights, termination rights, rights and obligations around exit and business continuity, and restrictions and controls around subcontracting.

[00:07:36.620] - Ian Duffy, Partner

Now, although compliance with the CBI outsourcing guidance will ultimately be the responsibility of the regulated firm that's contracting with a Fintech provider, it's still important that a Fintech provider is familiar with the guidance and they can look to develop template forms of customer contracts that they can use with regulated customers that cover the requirements of the guidance so that include those prescribed contractual provisions and that can be beneficial and help smoothen out the contracting process, as opposed to simply looking to negotiate in specific provisions to cover off the CBI outsourcing guidance on a case by case basis.

[00:08:14.110] - Ciara Anderson, Senior Associate

Thanks, Ian, that makes sense. So I know another evolving area on the regulatory landscape that we wanted to discuss is operational resilience. In particular, we want to talk about the Digital Operational Resilience Act, which we've referred to as DORA. So this was recently finalised in the EU in December, but it's due to come into force in the not too distant future. So do you want to talk a little bit about the relevance of DORA to Fintech providers?

[00:08:41.070] - Ian Duffy, Partner

Yeah, absolutely. Thanks, Ciara. So, as you touched on, DORA is focused on operational resilience in the financial services sector and as part of the European Commission's broader digital finance strategy and DORA is designed really to uplift existing ICT risk management requirements and existing requirements around operational resilience that apply to certain regulated firms and consolidate them into a single legislative instrument. Now, what's quite interesting about DORA is that not only will it apply to a reasonably broad range of regulated firms, so credit institutions, banks, insurance undertakings, investment firms, it will also apply to certain major ICT service providers, and this could include some large Fintech providers. Now, what this will mean in practice is that if a fintech provider is designated as critical to the proper operation of the financial sector in the EU by European financial regulators, it will be

subject to direct supervision by European financial regulators for the very first time. Now, providers that receive that critical designation will be assigned a European financial regulator who will assess whether that provider has a comprehensive and effective framework in place to be operationally resilient and to manage the risks that it poses to regulated firms in the EU from an IT perspective.

[00:09:59.730] - Ian Duffy, Partner

And that lead regulator can also issue recommendations to the provider and requires to take certain remedial actions. So, for example, it could insist that the ICT service provider, the fintech provider, includes certain provisions in its contract with its EU regulated customers, or it could impose certain restrictions around how that provider can subcontract. So it really is worthwhile for larger Fintech providers to start considering whether they might actually be designated as critical under DORA, and therefore be subject to direct supervision and oversight under DORA and as part of that, start to think about, well, do they have robust information security and operational resilience policies and procedures and measures in place, and also start to think about their contracts with their customers that will be subject to DORA. Like the outsourcing rules DORA prescribes that certain provisions need to be included in the contract between the regulated firm and the ICT service provider. So again, Fintech providers that work with lots of regulated firms might want to think about updating template contracts to include provisions for compliance with Dora. In terms of timing of DORA, it's due to come into effect on the 17th January 2025 so businesses do have some time to take steps necessary to align with DORA, but obviously, the sooner you start doing that, the better outcome from a compliance perspective.

[00:11:22.400] - Ian Duffy, Partner

So we've discussed DORA, we've talked about NIS 2, which are key new legislative developments in the information security and operational resilience space but there's also quite a lot happening around AI. So, Kira, do you want to discuss the AI Act, as it's extremely topical at the moment?

[00:11:39.310] - Ciara Anderson, Senior Associate

Absolutely and obviously there's been a lot of talk about the AI Act recently. I think it's probably important to focus on its main aim. So its main aim really is to regulate AI systems that are deemed to be high risk to you or me. So, for example, this will include AI systems that are a safety component in an already regulated product, such as a medical device. It also includes AI systems that are used to make decisions relating to an individual's employment, such as hiring or terminating employment but from a Fintech provider's perspective, it also includes systems that are used in the context of risk assessments for pricing life and health insurance, and also for AI systems that are quite common, which are used to evaluate an individual's credit score or credit worthiness so those will be brought within scope. However, it's probably important to clarify that most AI systems are not actually high risk. So, for example, in the Fintech sphere, it's unlikely that AI systems used to flag fraudulent transactions, for example, or to verify customer IDs will be considered high risk, and therefore most of the obligations under the AI Act will not apply to those systems.

[00:12:49.590] - Ciara Anderson, Senior Associate

Although again, caveat to that is there is an umbrella requirement, basically for all AI systems that the provider makes known to the user that they're engaging with an AI system. So that's just a minimal transparency requirement. In terms of the obligations that apply to high risk AI systems, these will include an obligation to conduct an appropriate risk assessment in order to identify any potential risks that the AI system may pose. So this is not dissimilar to the obligation to undertake a data protection impact assessment under the GDPR for example. Providers will also need to have very good data governance practises in place in relation to the data sets that they use to train their models. They'll also need to ensure that they have comprehensive documentation as to how the AI model ultimately works and makes decisions, because the Fintech provider will need to provide this information to their customers and ultimately to the end user to explain how the system works and finally, there is a requirement to undertake a conformity assessment with regard to quality management and the technical documentation underlying the system. There's been a lot of back and forth on the AI Act.

[00:13:58.490] - Ciara Anderson, Senior Associate

as I assume everyone knows, there was a particular reaction to Chat GBT which drove some further amendments. Although it looks like we're thankfully reaching the end of the road, it looks like it'll be finalised this summer and its provisions will apply 24 months later. So it's looking like Q3 2025.

[00:14:15.010] - Ian Duffy, Partner

Okay, that's great, Ciara, thanks. I think it'd be really interesting to see where ultimately the EU lands on the final text of the AI Act in the coming months and as you said, it looks like we're nearly there, so we'll have clarity on that soon and ultimately it'll be very interesting to see how the new legislative regime will play out in practice and of course, we'll be working closely with clients to assist them on the AI Act over the coming years. So that's it really, from us. We hope you found the podcast to be helpful. Just to summarise. So Fintech providers should continue to be mindful of their existing obligations in areas like data protection under NIS Directive and the impact of the CBI outsourcing guidance in terms of what to look for in the future, keep an eye out and keep your mind focused on DORA and NIS2 and then, a bit further down the tracks, the AI Act as well. So, like I said, that's it, and thank you for listening.