

WIKBORG | REIN

Update

February 2024

Compliance

The Crackdown on Price Cap Evasion

Page 4

Expansion of the UK's corporate criminal liability regime

Page 10

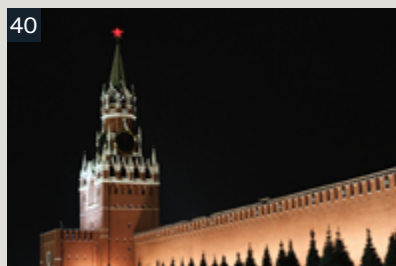
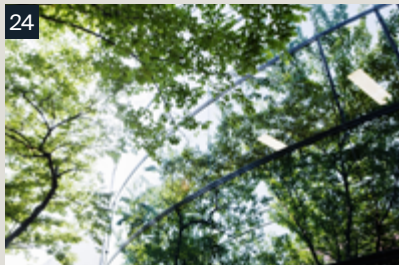
EU takes steps to empower consumers for the green transition

Page 20

Content

Compliance Update

The Crackdown on Price Cap Evasion and the BIMCO Russian Oil Price Cap Scheme Clause for Charter Parties	4
Managing cyber risk	8
Expansion of the UK's corporate criminal liability regime	10
Enforcing an award contrary to sanctions, an issue of 'public policy'?	14
China expands legislation for private sector corruption	18
EU takes steps to empower consumers for the green transition	20
EU agreement on corporate due diligence rules to safeguard human rights and environment	24
Proposed changes to Norway's foreign investment control regime	28
Two years following the invasion of Ukraine – some lessons learnt	32
Towards safe, reliable and human-centred AI	36
Are all state-owned Russian companies controlled by President Putin?	40
How to navigate China's anti-sanctions laws amidst the sanctions against Russia	44
Status: Mandatory human rights and environmental due diligence	48
Wikborg Rein's compliance practice – contact list	50



Update

February 2024

Publisher:
Wikborg Rein

Editors:
Tine E. Vigmostad, Kristin N. Brattli, Hanne R. Gundersrud

Photos:
gettyimages.com

Layout:
Helene S. Lillebye-Teien

Print:
Bodoni / 100 copies



UPDATE FEBRUARY 2024 COMPLIANCE

This Update is produced by Wikborg Rein. It provides a summary of the legal issues, but is not intended to give specific legal advice. The situations described may not apply to your circumstances. If you require legal advice or have questions or comments, please contact your usual contact person at Wikborg Rein or any of the contact persons mentioned herein. The information in this Update may not be reproduced without the written permission of Wikborg Rein.

Dear readers

Welcome to the first edition of the Wikborg Rein Compliance Update. The aim of this publication is to provide our readers with information and updates on current topics in ethics, compliance and crisis management.

It has now been two years since the Russian invasion of Ukraine. One of the ways the global community has responded has been to impose on Russia some of the most stringent and comprehensive sanctions ever imposed on a single country. In this edition, you will find several articles on sanctions-related issues, including some 'lessons learned' after the past few years of sanctions, how to navigate China's anti-sanctions laws amidst the sanctions against Russia and a contemplation on the issue of enforcement of arbitral awards that may contravene applicable sanctions.

As the regulatory landscape develops, compliance becomes increasingly important in more and more areas. This also includes the transition from hard law to soft law in several fields. One such area is responsible business practices and human rights. In this regard, the proposed new EU directive on corporate sustainability due diligence, which the Council of the European Union will vote on 9 February 2024, could be an historic breakthrough in the way companies can be held responsible for human rights abuses in their value chain. Furthermore, we have included an article on stricter EU marketing rules seeking to empower consumers for the green transition, which includes a ban on greenwashing.

This edition also covers updates within the wider compliance sphere, for example articles on the EU's Artificial Intelligence (AI) Act, managing the risk of cyberattacks and measures to better safeguard national security interests through potential changes to Norwegian foreign direct investment legislation.

In these ever-changing times, we hope you find our Compliance Update an enjoyable and informative read.



Elisabeth

Elisabeth Roscher

Partner and head of Wikborg Rein's ESG, Compliance and Crisis Management team, Oslo



As the regulatory landscape develops, compliance becomes increasingly important in more and more areas.

Editors of the Compliance Update



Tine E. Vigmostad
Partner
tvi@wr.no



Kristin N. Brattli
Partner
knh@wr.no



Hanne R. Gundersrud
Senior Lawyer
hgu@wr.no

The Crackdown on Price Cap Evasion and the BIMCO Russian Oil Price Cap Scheme Clause for Charter Parties

The BIMCO Russian Oil Price Cap Scheme Clause was long-anticipated when it was published on 2 June 2023. There has since been growing concern that the original Price Cap Measures were easy to circumvent, and in this article we examine the impact of the latest measures to combat such evasion.

The “Price Cap Measures” on Russian origin crude-oil and petroleum products (“**Russian Oil**”) were first introduced by the G7 countries and their coalition partners with effect from December 2022 and February 2023, respectively. Although there are subtle differences in the formal implementation of the scheme in the various participating countries, the essence is consistent: (i) a prohibition on marine transport, and services supporting such transportation, of seaborne Russian Oil globally, combined with an exception permitting the provision of such services if (a) the Russian Oil was purchased at or below a fixed price cap or (b) the party has reasonably relied on an attestation to that effect.

By now, shipping parties have already grown accustomed to the process of requesting price information and making attestations to comply with the Price Cap Measures. There has also been strong engagement by the industry and by lawyers specialising in shipping sanctions with the relevant sanctions authorities. This has resulted

in useful updates to the official guidance, as well as practical work to implement the rules.

Despite such successes, there has been growing unease that the Price Cap Measures might have been too easy to circumvent for illegitimate actors and have thus not been wholly successful in reducing the amount of non-Price Cap compliant trade in Russian Oil. As a result, the Price Cap Coalition recently agreed on a set of measures aimed at reducing circumvention, including more detailed attestation requirements. We have also seen high-profile enforcement action targeting some actors paying lip-service to the pre-existing position that adequate due diligence has to be carried out before relying on attestation and re-emphasising that attestations are not a “tick-box”-exercise.

ADDITIONAL ATTESTATION REQUIREMENTS

On 20 December 2023, [the Price Cap Coalition published a statement](#) outlining changes to the Price Cap Measures. As a result, all G7 countries and their coalition part-

ner service providers are required to “*receive attestations from their counterparties each time they lift or load Russian oil*”, also known as a per-voyage attestation requirement.

The relevant authorities in the EU, UK and US have published guidance elaborating on the content of the per-voyage attestation requirement. In short, Tier 1 and certain Tier 2 operators must provide an attestation confirming price cap compliance to any other Tier 1 or Tier 2 counterparty prior to the lifting or loading of Russian Oil or the effective date of the contract (whichever is earlier), and an additional attestation prior to the lifting or loading of Russian Oil. Further, they must provide an attestation to any Tier 3A operator (omitting reinsurers and certain financial institutions) prior to the effective date of the contract, and an additional attestation for every relevant voyage within 30 days of lifting or loading Russian Oil. Tier 3A operators must similarly request an attestation for all relevant voyages within 30 days of lifting or loading Russian Oil.

The per-voyage attestation



requirements enter into force on 19 February 2024 in the UK and US, and 20 February 2024 in the EU.

In addition to the per-voyage attestation requirements, the Price Cap Coalition requested that all operators with access to price information (Tier 1 and certain Tier 2 operators) maintain and retain itemised price information for ancillary costs, including e.g., cost of export licences, inspection, shipping fees and packaging. This information must be shared with operators without access to price information (Tier 3A operators and certain Tier 2 operators) upon request.

This requirement enters into force on the same date as the per-voyage attestation requirement set out above.

THE BIMCO CLAUSE

Since its introduction, the BIMCO Clause has been much used by shipping operators worldwide. The need for a specific clause on the Price Cap Measures was clear and, prior to its introduction, the industry's approach consisted of a number of bespoke clauses in circulation,

which in some cases resulted in fairly intense negotiations between counterparties.

The BIMCO Clause has been a useful and in many cases suitable clause to replace the pre-existing versions that we have seen in circulation.

However, the clause was drafted as a 'one size fits all' clause covering all Price Cap Measures for both time and voyage charters, and could not be expected to address all of the nuanced issues that arise in practice. As demonstrated by the tightening of the attestation requirements, one

of the issues in respect of long-term charters will be to ensure the clause is sufficiently "future proof".

Users should therefore carefully consider what changes are necessary to make the clause suitable for their purposes. Some important points to consider are:

1. The official EU and UK guidance on the Price Cap Measures makes it clear that owners must carry out sufficient due diligence to satisfy themselves that it is reasonable to rely on the price information / attestations provided



The per-voyage attestation requirements enter into force on 19 February 2024 in the UK and US, and 20 February 2024 in the EU.

by charterers. This may require owners to review additional information beyond what they are entitled to request under the BIMCO clause. Owners should consider whether they are sufficiently protected on this point by any charter party clauses or if they are comfortable on the basis of their pre-existing knowledge of the charterers or trading in question.

2. It may be beneficial to both parties to include some form of “pre-approval” process where owners can assess the relevant trade, the parties involved and agree what further information will be received. This can help avoid situations where it is discovered at a late stage that owners are unable to satisfy themselves of the above requirements, which can cause delays and lead to conflicts. For charterers, this may be especially important in a charter party where owners have other relevant rights to refuse orders.
3. Owners should also consider whether the general confirmation that charterers are complying with their own reporting requirements is sufficient. For example, the UK Price Cap Measures require owners to report to OFSI if owners transact directly with a Tier 1 counterparty in certain circumstances, including when that Tier 1 counterparty is not itself required to report because UK sanctions

do not apply to it. Accordingly, if UK owners are dealing with charterers who are also the buyer or seller of the cargo, it will be important for owners to find out if charterers are actually reporting to OFSI.

4. The new requirement for a voyage-based attestation is largely covered by the requirement to provide an attestation “*prior to each loading of any Price Cap Cargo*”. However, there is a nuance in the EU guidance requiring a new attestation before any ship-to-ship operation.
5. The clause also does not expressly take into account the mandatory requirement for Tier 1 and Tier 2 operators, which will usually include charterers, to collate and keep itemised cost information upon request. Wording to that effect is not included in the standard attestation language. The provision allowing owners to request evidence from charterers arguably only covers evidence that charterers already hold.
6. While arguably these “new” concerns are implicitly covered by the general warranty given by charterers that all employment will comply with the Price Cap Measures, dealing expressly with these issues is likely to reduce the scope for conflict. Owners may also want to consider whether they will be in a position to comply with their insurers’ requirements, which may be more

stringent than strictly required by the Price Cap Measures.

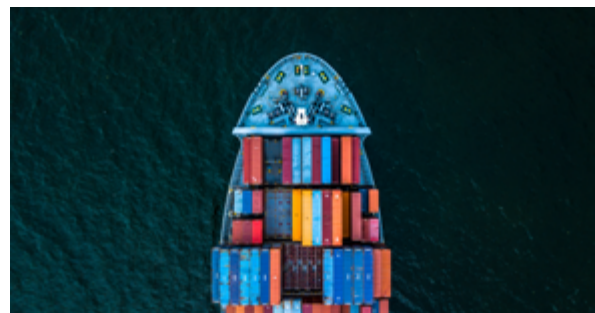
7. Owners and charterers should also carefully review the rights and remedies in sub-clause (e) of the BIMCO Clause and consider if these are suitable for their specific charter party. We comment further on this point below.

In relation to the last point regarding remedies, this is an issue that we have commented on in our more general sanctions articles in the context of longer-term contracts (available at [wr.no](#)). In the context of the Price Cap Clause, it is worth keeping in mind that:

- For owners, the main point will be whether the indemnity adequately covers their interests. The indemnity as drafted only covers losses arising from a breach, and as such may not extend to any steps taken by owners on the basis of having reasonable grounds to suspect activity contrary to the Price Cap Measures. Owners might therefore find themselves unable to pass on a loss for actions reasonably taken in response to a suspected breach of the Price Cap Measures.
- Charterers should note that owners are given the right to terminate the charter party in case of a breach of the clause and where owners have reasonable grounds to suspect activity contrary to the Price Cap Measures.



There has been growing unease that the Price Cap Measures might have been too easy to circumvent for illegitimate actors.



- More generally, the cause of breaches or the grounds for suspicion may be outside of charterers' control. Charterers may therefore find it difficult to accept such a wide right to terminate if it is a long-term charter party that is crucial to their business. Additional flexibility may be appropriate in such cases if the breach can be

remedied or if performance can be lawfully altered in some way.

In our experience the BIMCO Price Cap Clause has been widely adopted both "as is" and as a starting point for negotiations. In light of the recent development signposting that the Price Cap Measures are still being refined and that addi-

tional changes to further promote transparency are foreseeable, we would welcome an update to the clause that will reduce the perceived need or desire for bespoke amendments. In the meantime, we do not expect operators to find it too challenging to update what remains a well-drafted clause with clear and concise language.

Contacts



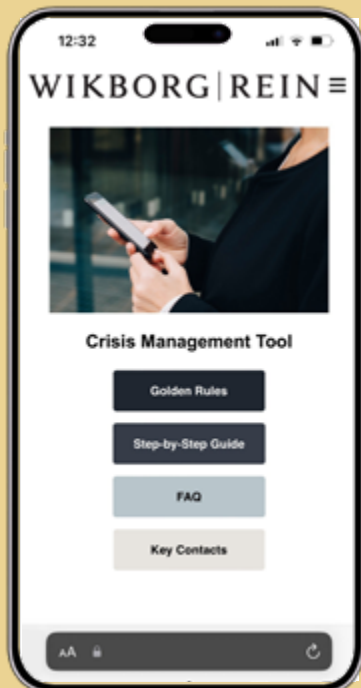
Tine E. Vigmostad
Partner
tvi@wr.no



Sebastian Sandtorv
Senior Associate
sbs@wrco.co.uk



Marie S. Hatten
Associate
mht@wr.no



Download our app!

Wikborg Rein's **Crisis Management Tool** is now ready for download. The tool provides practical, immediate and step-by-step guidance in case of various types of crises arising as a result of unannounced inspections and controls by the police or other public authorities

You can download the app by scanning the QR code and register



Managing cyber risk

All companies face the risk of cyber-attacks. In general, the question is *when* and not *if* an attack will strike. Companies should therefore strengthen their cyber resilience and implement robust measures to be prepared to handle all aspects of an attack if/when it occurs.

In this article we give a brief overview of some of the latest developments in Norway in the area of cyber risk and cyber legislation, and share some recommendations for how companies should prepare to manage this risk going forward.

CYBER SECURITY MUST BE PRIORITISED

The latest annual report on national digital risk in Norway was published by the Norwegian National Security Authority (“NSM”) on 19 October 2023 [*Nasjonalt digitalt risikobilde 2023 (nsm.no)*]. The purpose of the report was to raise awareness and motivate enterprises to increase their cyber security efforts, with NSM generally emphasising that both public and private enterprises must prioritise cyber security going forward.

The report highlights the following key points:

- The developments in artificial intelligence, including large language models, are expected to lead to further professionalisation among attackers.
- Cyber-attacks can have an increased physical impact as industrial systems (such as those linked to critical infrastructure) are increasingly connected to the internet.

- Increased focus on cyber security may make other methods of accessing information more attractive to malicious actors. The risk from insiders to the system may increase with a one-sided focus on cyber security. Thinking about security in all domains is crucial.
- Cyber-attacks aimed at influencing voters place a strain on democracies.

Based on the ever-increasing risk, cyber security is a topic that should be high on the agenda both for company boards and management. Directors and managers must recognise the importance of understanding how cyber risk can threaten the values of the company, take necessary measures to ensure the continued operation of the business (in the wake of a cyber-attack), mitigate financial loss, prevent loss of confidential information / personal data and limit the risk of liability and reputational damage. Pursuant to the Companies Act, Norwegian boards have a duty to familiarise themselves with and follow up on potential compliance risk areas for the company. The board sets expectations and partially sets guidelines for management priorities. Additionally, board members may be held personally liable (by shareholders) in the event of financial loss.

EU CYBER SECURITY DIRECTIVES AND CORRESPONDING LEGISLATIVE DEVELOPMENTS IN NORWAY

With respect to cyber legislation, there is a steady stream of developments which companies must take into account in their efforts to implement comprehensive and good cyber management.

In Norwegian law, the latest development is the Norwegian Parliament’s adoption of the Digital Security Act on 20 December 2023. The act incorporates the EU’s cyber security directive, the NIS1 Directive (albeit that its date of entry into force has not yet been determined). The Digital Security Act requires organisations that have a particularly important role in maintaining critical social and economic activity to comply with digital security requirements and to notify authorities of serious digital incidents. A number of industries /sectors have already been subject to legal requirements for digital security for a number of years, including in particular the financial and health sectors. The new legislation will therefore have particular significance mainly for companies in industries that have not previously been subject to equally extensive requirements for digital security.

In the EU, the second iteration of the cyber security directive – NIS2 –

has already entered into force. NIS2 imposes security requirements, as well as incident notification and governance obligations on entities in a range of critical sectors, including energy, transport, finance, health, and digital infrastructure. Member states have until October 2024 to transpose the directive into national law. In addition to mitigating certain weaknesses in NIS1, the NIS2 Directive aims to expand and harmonise the scope of the cyber security rules while also setting certain minimum requirements. It is not certain when NIS2 will become part of Norwegian law. However, it is possible that the Norwegian government will look to the NIS2 Directive's obligations and scope when drawing up regulations under the already adopted Digital Security Act.

Regardless, companies should even now take account not just of NIS1, but also of the requirements set out in the NIS2 Directive. Even Norwegian companies without operations in the EU may be indirectly affected by NIS2, since customers subject to the requirements in NIS2 to a greater extent than under NIS1 will be obliged to follow up on cyber risk and resilience in their supply chains.

In addition, companies must be cognisant of the numerous other relevant legal requirements pertaining to cyber security, including (but not limited to) information security requirements. This includes general laws such as the Security Act, which applies to national security, and the Personal Data Act, which applies to the protection of personal data. There are also requirements that apply to specific industries or products, such as sector specific regulations in finance, health and the public sector. Additionally, the upcoming Cyber Resilience Act is highly relevant. This will be the first EU-wide legislation of its kind, introducing common cyber security rules for manufacturers and devel-

opers of products with digital elements, covering both hardware and software.

CYBER RISK MANAGEMENT AND INCIDENT HANDLING

Preparation is key to managing cyber risks and limiting the disruption and damage that cyber security incidents cause. Such preparedness can for example be achieved by:

- setting up a risk-based cyber security risk management programme, implementing governance-, compliance- and contractual measures;
- identifying applicable regulatory requirements, including notification requirements;
- implementing an effective Cyber Incident Response Plan, which establishes a written systematic approach to handling the incident and includes detailed procedures/guidelines (e.g. checklists), stakeholder management etc.;
- conducting awareness and preparedness training;
- mapping and following up on employee risks (insider threats etc.);
- setting up a dedicated data breach response procedure pursuant to the GDPR;
- mapping risks related to liability in relevant vendor and customer contracts; and
- assessing cyber insurance issues.

In the event of a cyber-attack, it is important to have a trusted partner that can assist in taking immediate and effective action. Wikborg Rein has extensive experience handling various types of incidents, including related to security breaches. We are also used to working seamlessly with technical experts who will play a central role in dealing with cyber risks and incidents as they arise.

Contacts



Gry Hvidsten
Partner
ghv@wr.no



Elisabeth Roscher
Partner
elr@wr.no



Based on the ever-increasing risk, cyber security is a topic that should be high on the agenda both for company boards and management.

Expansion of the UK's corporate criminal liability regime

The UK Economic Crime and Corporate Transparency Act 2023 (“the ECCTA”) was formally approved on 26 October 2023. Among the most significant reforms introduced by the ECCTA are the establishment of ‘failure to prevent fraud’ as a new UK corporate criminal offence, and a reform of the UK identification doctrine expanding the extent of corporate criminal liability for economic crimes. In this article, we highlight the details of these two key aspects of the Act, and explain how they will affect Norwegian companies with operations or subsidiaries in the UK.


The [Economic Crime and Corporate Transparency Act](#) is the latest piece of legislation introduced by the UK Government to combat economic crime and strengthen corporate transparency. It builds on, and supplements, the Economic Crime (Transparency and Enforcement) Act 2022, which created a Register of Overseas Entities, reformed the UK unexplained wealth order regime and allowed the UK Government to act more efficiently when imposing sanctions. The ECCTA expands on the transparency, corporate liability and sanctions reforms introduced by its predecessor.

As we will explain further below, the amendments introduced by the ECCTA, the application of which is in part extra-territorial, are relevant for Norwegian companies with UK subsidiaries or operations.

This article will focus on the expansion of corporate criminal liability through the ECCTA's introduction of the ‘failure to prevent fraud’ offence and reform of the identification doctrine (the manner for attributing corporate criminal liability under English law). In addition to these reforms, we briefly mention that the ECCTA contains several requirements relating to the registration of companies in the UK, including to enhance the powers of the UK Companies House, introduce new company registration requirements and identity verification requirements for company directors and people with significant control, and increase the transparency of ownership and governance of UK corporate entities.

‘FAILURE TO PREVENT FRAUD’ AS A NEW CRIMINAL OFFENCE

The ECCTA introduces ‘failure to prevent fraud’ as a criminal offence for companies and partnerships (together referred to as ‘organisations’). The offence builds on existing offences such as the failure to prevent facilitation of tax evasion under the UK Criminal Finances Act 2017 and failure to prevent bribery under the UK Bribery Act 2010. As with these offences, the failure to prevent fraud offence applies across all commercial sectors. However, unlike the pre-existing ‘failure to prevent’

 **Norwegian companies with UK operations could be liable if an associated person commits fraud or an essential element of fraud in the UK, or if some harmful impact of the offence is felt in the UK.**



offences, the offence under the ECCTA is limited to 'large organisations'.

Section 201 of the ECCTA defines 'large organisations' as bodies that satisfy at least two of the following three conditions in the financial year preceding the fraud offence:

- i. More than £36 million turnover
- ii. More than £18 million in total assets on the balance sheet
- iii. More than 250 employees

Pursuant to Section 202, the offence also applies to parent companies (including non-UK parent companies, if there is UK nexus) if the group satisfies, in aggregate, at least two of the following three conditions in the financial year preceding the fraud offence:

- iv. More than £36 million net (or £43.2 million gross) turnover
- v. More than £18 million net (or £21.6 million gross) in total assets on the balance sheet
- vi. More than 250 employees

It is possible that the scope will expand in the future to include small and medium sized enterprises (SMEs), since the thresholds can be amended by secondary legislation.

Importantly, the failure to prevent fraud offence has a wide extra-territorial application. [The UK Government's Factsheet](#) about the new offence states that if an employee commits fraud under UK law, or targeting UK victims, the employer could be prosecuted, even if the organisation or the employee is based overseas. Since most of the listed offences already have a wide extra-territorial application, Norwegian companies with UK operations could be liable if an associated person commits fraud or an essential element of fraud in the UK, or if some harmful impact of the offence is felt in the UK (e.g., the offence targets UK victims).

For organisations to be liable for the failure to prevent fraud, three conditions must be present:

- i. a specified economic offence must be committed by an 'associated person', i.e. an employee, agent or subsidiary of

- the organisation, or a person that otherwise performs services for or on behalf of the body
- ii. the offence must be intended to benefit, directly or indirectly, the organisation or any person to whom the organisation provides services (e.g. customers or clients)
 - iii. the organisation must not have had reasonable fraud prevention procedures in place.


The term ‘associated person’ is defined broader in the ECCTA than its counterparts in the failure to prevent bribery and failure to prevent facilitation of tax evasion offences. Under the latter offences, subsidiaries and employees will only be ‘associated persons’ if they perform services for or on behalf of the organisation (albeit that there is a (rebuttable) presumption that employees will be considered associated persons of their employer company). In contrast, all subsidiaries and employees are automatically considered ‘associated persons’ by virtue of section 199(5) of the ECCTA. It remains to be seen whether these distinctions in the respective legislative texts – which may create problems in practice if equivalent terms are given different meanings – will remain once the government guidance on the failure to prevent fraud offence is published.

Liability is not dependent on the company being aware of the fraud. Nonetheless, the organisation will not be liable if it was, or was intended to be, a victim of the fraud offence. This concession only applies where the offence was intended to benefit a client or customer of the organisation, and not where it was intended to benefit the organisation.

The UK government will publish a list of economic offences to which the duty to prevent fraud will apply. The list will include false accounting, as well as core offences under the UK Fraud Act 2006, such as false representation, failure to disclose information and abuse of position. Additionally, obtaining services dishonestly, participation in a fraudulent business, fraudulent trading, false statements by company directors, and cheating the public revenue will be covered. Money laundering will not be considered an offence under the new provision, as legislators considered it already addressed by existing regimes. Further offences can be added by secondary legislation, provided that they involve ‘dishonesty’, are of a similar character to those listed, or are relevant money laundering offences under Section 327 to 329 of the Proceeds of Crime Act 2002 (concealing, arrangements, and acquisition, use and possession).

Moreover, the failure to prevent fraud offence also includes ‘aiding, abetting, counselling or procuring the commission of a listed offence’. Thus, a company could be liable in cases in which an employee has assisted another entity in committing an offence intended to benefit the company or its clients.

Organisations will benefit from a defence to the failure to prevent fraud offence if they can prove that they had reasonable procedures in place to prevent the fraud, or that it was not reasonable to expect any prevention procedures to be in place. This must be decided in light of ‘all the circumstances’. The Act’s use of the term ‘reasonable procedures’ reflects the recent shift in the UK legal landscape – including by the House of Lords Bribery Act 2010 Committee and the UK Law Commission – from a requirement that prevention procedures should be ‘adequate’, to the expectation that they must be ‘reasonable’. This, in turn, reflects a fear that the term ‘adequate’ would be interpreted so strictly that no defendant company would be able to avail itself of the defence. The Government is required to issue guidance about procedures which are considered reasonable in this regard, and such guidance is expected to be published in spring 2024.

 **To make it easier to prosecute companies for criminal wrongdoing, and aiming to establish a more effective deterrent, the new law expands the extent to which companies and partnerships can be held criminally liable for economic crimes.**

Based on the UK Government's guidance to the failure to prevent bribery and failure to prevent facilitation of tax evasion offences, it is expected that the guidance may cover the following topics:

- Having in place proportionate procedures to prevent economic crimes
- Top-level commitment to preventing bribery by associated persons
- Undertaking periodic, informed and documented risk assessments
- Implementing due diligence procedures
- Communication and training
- Monitoring and review of procedures designed to prevent fraud

The failure to prevent fraud offence is expected to enter into force after the UK Government's guidance on reasonable procedures has been published. If convicted, the organisation is liable to a fine, a limit for which is not stated in the ECCTA.

REFORM OF THE IDENTIFICATION DOCTRINE EXPANDING CORPORATE CRIMINAL LIABILITY FOR ECONOMIC CRIMES

The identification doctrine entails that where a specific mental state (e.g. intent, dishonesty or recklessness) is a prerequisite for an offence, a company would only be liable if a person representing the 'directing mind and will' of the company possessed the required mental state. This evidential hurdle has proved challenging for prosecutors in practice, however, in particular with respect to larger organisations (as also illustrated by a number of high-profile prosecutorial failures by the UK's Serious Fraud Office in later years). To make it easier to prosecute companies for criminal wrongdoing, and aiming to establish a more effective deterrent, the ECCTA expands the extent to which companies and partnerships can be held criminally liable for economic crimes. This expansion entered into force on 26 December 2023.

Under Section 196 of the ECCTA, organisations will be guilty of a 'relevant offence' committed by a 'senior manager' acting within the actual or apparent scope of their authority. This also applies where the senior manager attempts or conspires

to commit an economic crime as defined in the Act. Unlike the 'failure to prevent fraud' offence, the reform of the identification doctrine applies to all companies regardless of size.

A 'senior manager' is defined as an individual who plays a significant role in:

- i. the decision-making about how the organisation's activities, or a significant part of the organisation's activities are to be managed or organised, or
- ii. the actual managing or organising of the whole or a substantial part of those activities

Schedule 12 of the Act contains a list of 'relevant offences' of an economic nature, including the offences covered by the failure to prevent offence, as well as others, such as money laundering, offences relating to sanctions and terrorist financing, and certain financial services offences under the Financial Services and Markets Act 2000.

In its [Factsheet](#) about the reform, the UK Government outlines its intention to extend the identification doctrine reform to all criminal offences in due course. This means that companies will need to put in place measures to prevent employees, agents, subsidiaries and other associated persons from committing a wider range of economic crimes than those covered by the 'failure to prevent fraud' offence.

If no act or omission forming part of the offence takes place in the UK, the organisation is only guilty of an offence if it would be guilty of the relevant offence in the country in which it was committed. Since most of the 'relevant offences' under the ECCTA are offences also under Norwegian law, the reform of the identification principle will also potentially affect UK subsidiaries of Norwegian companies, even where the offence itself is committed in Norway, provided there is still some form of UK nexus / involvement of the UK subsidiary. It is worth noting, however, that Norwegian law already allows for attribution of corporate liability where an offence has been committed by a senior manager who has acted on behalf of a company, and this concept as such should therefore already be well-known to Norwegian entities.

Contacts



Elisabeth Roscher
Partner
elr@wr.no



Kristin N. Brattli
Partner
knh@wr.no



Hanne R. Gundersrud
Senior Lawyer
hgu@wr.no



Mads K. Haugse
Associate
mau@wr.no

Enforcing an award contrary to sanctions, an issue of 'public policy'?

The past few years have illustrated with a vast intensity the relevance of international sanctions for an ever expanding number of businesses and sectors. This backdrop has also led to a significant increase in sanctions related disputes, which in turn has led to discussions regarding enforcement of arbitral awards that contravene applicable sanctions.

“ Companies with assets in countries outside the EU may find that an arbitral award may be enforced by seizure of these assets, even in the event that the arbitral award is not enforceable in the EU.

Violations of sanctions can lead to a wide array of adverse consequences, including civil and criminal liability. The list of trading restrictions is continuously expanding. This is the backdrop to the challenging balancing act market operators are facing between ensuring sanctions compliance and continuing commercial operations, while avoiding legal disputes with counterparties as a result of having taken an overly restrictive approach to sanctions compliance.

Arbitral awards are as a starting point valid and binding, and should be complied with. However, the arbitral award may mandate that a party undertakes a transaction that the arbitral tribunal wrongfully has found not to be a contravention of sanctions, or that has become prohibited by sanctions after the award is rendered, or enforcement may be sought in a jurisdiction other than that of the law of the contract or the seat of arbitration. In such instances, the party obliged by the award may be in breach of sanctions by complying with the award, in turn risking civil and criminal penalties. The party may, therefore, wish to oppose enforcement of the award.



CAN SANCTIONS COMPLIANCE AMOUNT TO 'PUBLIC POLICY'?

Under the New York Convention [United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958)], Article 5 (2) (b), the recognition and enforcement of an arbitral award may be refused if the competent authority in the country where recognition and enforcement is sought finds that the recognition or enforcement of the award would be contrary to the public policy of that country. (Most international arbitration conventions and national arbitration statutes are modelled on this provision, including Norwegian law.) What constitutes 'public policy' is narrowly construed; it is commonly not sufficient that the arbitral award runs contrary to mandatory laws and regulations. Generally, the 'public policy' argument is meant to be used to set aside an award or refuse its enforcement if it breaches fundamental rules or principles of a material or procedural nature. Enforcement may only be denied where it would violate the forum state's most basic notions of morality and justice [See for example

Parsons & Whittemore Overseas Co., Inc. v. Société Générale de l'Industrie du Papier (RAKTA), U.S: Court of Appeals, 2d Cir., Dec. 23, 1974, 508 F.2d at 973-974 and *IPCO (Nigeria) Ltd v. Nigerian National Petroleum Corp.* [2005] EWHC 726], which should not be equated with the state's foreign policy. This strict approach recognises the finality of arbitral awards, and is internationally adopted.

This gives rise to the question of when rules on economic sanctions and restrictive measures are sufficiently fundamental to be considered 'public policy', paving the way for a refusal to enforce arbitral awards in breach of them. In *Eco Swiss* [C-126/97] the Court of Justice of the European Union stated that the current Article 101 Treaty on the Functioning of the European Union (TFEU), prohibiting anti-competitive behaviour, constituted a fundamental provision for the functioning of the EU internal market, thus being EU public policy. This has been repeated in later case law. As such, it may well be argued that EU sanctions should be treated in the same manner – at least as a starting point – within EU member states [See e.g. *Government*

& *Ministries of the Republic of Iraq v. Armamenti e Aerospazio SpA et al.* and CAM Case No. 1491, Award of the Chamber of Arbitration of Milan, 20 July 1992, cited in XVIII *Yearbook of Commercial Arbitration* 1993 80.] and Norway (where implemented into Norwegian law), since they ‘represent the fundamental objectives and values of the EU’ [Szabados, ‘EU Economic Sanctions in Arbitration’. *Journal of International Arbitration* 35, no. 4 (2018): 439–462.].

For companies whose assets are primarily located in Norway or the EU, sanctions might therefore prevail in the case of a conflict with the arbitral award. Such companies wishing to make a transaction with a sanctioned party in order to comply with an arbitral award must therefore seek authorisation from relevant authorities to do so (this would also be the case for the settlement of an award). In the absence of such authorisation, companies may resist enforcement of an award by arguing that this would be contrary to public policy, and that enforcement should therefore be refused or postponed until the applicable sanctions are repealed. Indeed, it has been argued that courts of EU member states must apply overriding provisions such as EU sanctions *ex officio*, i.e. without the parties needing to raise the objection [Kunda, *Internationally Mandatory Rules of a Third Country in European Contract Conflict Laws* (Rijeka Law Faculty 2007) 132 and Otelnikov, ‘Economic sanctions, arbitrability and public policy’. *International Arbitration Law Review* (2020), 19–30].

Whether this is the case also outside Norway or the EU, or indeed for sanctions imposed by other regimes, must be subject to further scrutiny. By way of illustra-

tion, in a judgment from the Paris Court of Appeal, *Sofregaz v. NGSC* [Decision No. 19-07261 of June 3, 2020], a distinction was made between UN and EU sanctions on the one hand and US sanctions on the other. The court held that UN Security Council Resolutions and EU sanctions regulations could form part of international public policy, since they were intended to contribute to international peace and security, although unilateral US sanctions did not. For an arbitral award to be set aside on such grounds, the court stated that a violation of international public policy must be concrete and effective. Hence, the case illustrates that courts need to assess the merits of each case to conclude on whether the enforcement of the arbitral award would indeed constitute a clear violation of any applicable sanctions and ‘public policy’.

Whether or not an arbitral award mandating a transaction to an entity or individual sanctioned by the EU will be enforced, will vary from jurisdiction to jurisdiction. Key factors to consider are the relevant jurisdiction’s public policies and recognition of the sanctions in question, whether the sanctions are imposed by international bodies or unilaterally, and whether the enforcement of the arbitral award would manifestly violate sanctions. While EU sanctions may be given prevalence by courts in Norway or the EU the question is largely unresolved, and companies with assets in countries outside the EU may find that an arbitral award may be enforced by seizure of these assets, even in the event that the arbitral award is not enforceable in the EU.

“ For companies whose assets are primarily located in Norway or the EU, sanctions might therefore prevail in the case of a conflict with the arbitral award.

Contacts



Aadne M. Haga
Partner
aha@wr.no



Tine E. Vigmostad
Partner
tvi@wr.no



Aksel Kolstad
Associate
ako@wr.no



Mads K. Hauge
Associate
mau@wr.no



China expands legislation for private sector corruption

China has amended its criminal law for the 12th time with effect from 1 March 2024 by increasing penalties and adding employees of private companies to some bribery and corruption offences that currently only apply to employees of state-owned enterprises.

The Standing Committee of the National People's Congress, China's legislative body, passed the 12th amendment ("**Amendment No. 12**") to the Chinese criminal code on 29 December 2023, with an aim to strengthen anti-corruption legislation in relation to employees of private companies. This aim aligns with that of the ongoing anti-corruption movement in China, which is expected to increasingly target sectors such as finance, pharmaceuticals and infrastructure.

EXPANDED SCOPE OF BRIBERY OFFENCES

A key aspect of Amendment No. 12 is an expansion of the scope of the bribery offences under articles 165, 166 and 169 to private companies. These articles apply to bribery by senior personnel that causes significant harm to the company and prohibit the following offences:

- Abuse of function by a director or manager operating a competing business to the one in which he is employed for personal gain (conflicts of interest) (Article 165).



Recently, the government has declared an intention to target not only high-profile cases, but also to root out smaller-scale corruption.

- Abuse of function by any employee taking advantage of their office for the benefit of relatives or friends (Article 166).
- Malpractice by a senior manager selling discounted company assets for personal gain (Article 169).

Previously, only employees in state-owned enterprises were referenced under these articles. Amendment No. 12 thus represents a shift towards more robust anti-bribery regulations in the private sector.

Amendment No. 12 aims to address some new situations and problems which have recently arisen in practice with regard to corruption crimes within private companies in China. Notably, there has been a rise in instances of bribery within private companies, which led legislators to consider that further strengthening of the criminal code was necessary.

TOUGHER PENALTIES FOR SERIOUS OFFENCES

Penalties for offences in respect of giving and receiving bribes have been revised with a general increase in penalties and minimum sentences for serious cases. Amendment No. 12 applies to the following articles of the criminal code:

- Article 387 on state agencies or state-owned enterprises receiving bribes.
- Article 390 on offering bribes.
- Article 391 on bribing state agencies or state-owned enterprises for illegitimate benefits.
- Article 393 on giving illegal rebates to state functionaries for illegitimate benefits.

In general, the maximum sentences have been amended to imprisonment for up to three years for most cases, and between a minimum of three years', up to a maximum of ten years' imprisonment in more serious cases. The maximum sentence for offering bribes under article 390 is still life imprisonment if the circumstances are especially egregious, and the possibility of criminal detention and fines in relation to certain offences are retained.

In addition to the amendments relating to sentencing, article 390 (related to offering bribes) has also been amended to clarify which aggravating factors merit increased punishment. These factors include repeat offences, bribing state functionaries, law enforcement or judicial officers, bribery in the commission of another offence, bribery in key national projects or to secure positions or promotions or change of positions, and use of illegal gains. Offering bribes in areas such as ecology and environment, financial and fiscal affairs, work safety, food and drugs, disaster prevention and relief, social security, education and healthcare shall also be subject to more stringent penalties. This list reveals the heightened importance placed on these areas by the Chinese government.

CHINA'S ANTI-CORRUPTION CAMPAIGN

Amendment No. 12 should be seen as part of the larger anti-corruption movement in China that has seen more than three million public officials punished for corruption since President Xi came to power. Recently, the government has declared an intention to target not only high-profile cases, but also to root out smaller-scale corruption among the so-called “ants and flies”: the lower ranking officials and more minor players.

China's anti-corruption campaign is considered popular domestically, and China has seen significant improvements over this period, climbing six points on Transparency International's Corruption Perceptions Index to a current score of 42 out of 100, although the country still scores below the current global average of 43 and the regional average of 45.

We expect anti-corruption to remain a top priority for China with heightened enforcement and further expansion of the legal framework already in place. As an example, on 24 October 2023, the Supreme People's Court published a verdict issued by Guangzhou Intermediate People's Court in Guangdong Province involving three bribes, amounting to 220,000 Singapore dollars, paid in the period from 2017 to 2019 by two employees working for the international business department of China Railway Tunnel Bureau Group Co., Ltd. to [public officials in Singapore](#). This is the first reported case of its kind and signals an increased willingness to enforce anti-corruption legislation beyond the domestic cases typically seen to date.

INTERNATIONAL COMPANIES

The upcoming changes highlight the need for good corporate governance in the private sector also for international companies. In this respect China aligns with international trends, including those in areas other than corruption, as heralded by the Norwegian Transparency Act and the upcoming EU regulations on supply chain due diligence. International companies can therefore expect their China operations to come under increased scrutiny, not only from authorities at home, but also from Chinese officials.



Notably, there has been a rise in instances of bribery within private companies, which led legislators to consider that further strengthening of the criminal code was necessary.

Contacts



Kristin N. Brattli
Partner
knh@wr.no



Bård B. Bjerken
Senior Lawyer
bbb@wrco.com.cn



Sherry Qiu
Senior Associate
shq@wrco.com.cn





EU takes steps to empower consumers for the green transition

Shielding consumers from greenwashing and misleading environmental claims constitutes an important aspect of the European Union's strategy to cultivate a more environmentally sustainable economy. A European Commission study in 2020 revealed that more than 50% of environmental claims within the EU were unclear or misleading, with 40% lacking substantiation.


Commencing in 2022, the EU has undertaken a revision of current legislation to enhance consumer empowerment in the realm of the green transition, focusing on fortifying protection against unfair commercial practices and augmenting informational resources. These regulatory adjustments collectively aim to furnish consumers with the means to make well-informed and environmentally conscious choices through better quality information.

From a business standpoint, the intention is that genuine efforts to enhance product sustainability will garner recognition and consumer reward, potentially leading to increased sales. This approach aims to create an equitable competitive landscape for the dissemination of environmental performance information for products.

PROVISIONAL AGREEMENT ON ENHANCED CONSUMER PROTECTIONS TOWARDS THE GREEN TRANSITION

On 17 January 2024, the European Parliament formally endorsed its provisional agreement with the Council on the Directive Empowering Consumers

for the Green Transition through Better Protection against Unfair Practices and Better Information (the “**Green Transition Directive**”). The new directive aims at enhancing consumer rights by amending two directives that protect the interests of consumers at Union level: the Unfair Commercial Practices Directive 2005/29/EC (UCPD) and the Consumer Rights Directive 2011/83/EU (CRD). The new directive is also meant to work together with the Green Claims Directive, currently being discussed at committee stage in the European Parliament. The CRD currently requires traders to provide consumers with information on the main characteristics of their goods and services. However, as there is no requirement

 **According to the Green Claims proposal, companies will have to back up environmental information with evidence.**

in the directive to provide information on the absence of commercial guarantees of durability, the CRD does not sufficiently incentivise producers to provide such guarantees to consumers. Furthermore, the CRD does not contain specific requirements to provide information to consumers on the reparability of goods. The Green Transition Directive would address these issues by ensuring that consumers are provided with information on the existence of a commercial guarantee of durability of more than two years, covering the entire product, whenever such information is made available by the producer, and with information on the reparability of products, through a reparability score or other relevant repair information, where available, for all types of goods.

The general rules in the UCPD on misleading practices can be applied to greenwashing practices when they negatively affect consumers, using a case-by-case assessment. However, neither the UCPD nor its Annex I (the blacklist) contain specific rules defining such practices as unfair in all circumstances. The Green Transition Directive aims to enhance the transparency and reliability of product labelling by prohibiting the utilisation of general environmental claims such as “environmentally friendly,” “green,” “natural,” “biodegradable,” “climate neutral,” or “eco” without substantiating evidence. Furthermore, the regulation will govern the use of sustainability labels to address the confusion stemming from their widespread adoption and inadequate reliance on comparative data. Henceforth, only sustainability labels rooted in official certification schemes or established by public authorities will be permissible within the

European Union. Moreover, the directive will ban claims that a product possesses a neutral, reduced, or positive impact on the environment due to emissions offsetting schemes.

To sum up, the Green Transition Directive aims to enhance consumer information and combat deceptive practices in marketing. This includes disclosing the producer’s durability guarantee for all goods, providing details on free software updates for digital products, and indicating product reparability through scores or relevant repair information. Traders are mandated to avoid misleading consumers on environmental and social impacts, durability, and reparability. Restrictions are placed on making future environmental performance claims without clear commitments and advertising common market practices as unique benefits. Comparisons between products are allowed only with transparent information, and the display of sustainability labels without certification is prohibited. The regulations also ban generic environmental claims without demonstrating excellent performance as per relevant regulations. Claims about the entire product are restricted to the specific aspect concerned. Additionally, presenting legal requirements as distinctive features and engaging in practices related to early product obsolescence are prohibited.

Given that the Green Transition Directive modifies prevailing EU consumer law directives, its provisions will benefit from the comprehensive array of enforcement mechanisms available in current EU consumer law, recently strengthened by the Better enforcement and modernisation Directive, the Representative Actions Directive and the Revised Consumer Protection Cooperation Regulation.

NEXT STEPS

Following the current stage, formal approval by the Council is required for the Green Transition Directive before it can be officially published in the EU’s Official Journal. Subsequently, member states will be allotted a 24-month period

 **Only sustainability labels rooted in official certification schemes or established by public authorities will be permissible within the European Union.**

to incorporate it into their national laws. Enforcement of these measures will take effect six months later, totalling 30 months from the directive's official commencement.

THE GREEN CLAIMS DIRECTIVE

In March 2022, the European Commission presented a draft proposal on the substantiation and communication of explicit environmental claims. The Green Claims Directive will complement the Directive on Empowering Consumers for the Green Transition, offering more specific conditions regarding the substantiation and communication of environmental claims. According to the proposal, companies will have to back up environmental information with evidence, as all claims they make about environmental aspects or performance of their products must be based on scientific and verifiable methods.

The scope of the proposed directive is so-called "explicit environmental claims" made by traders about products or traders in business-to-consumer commercial practices, except those already regulated by other EU regulations. The latter means that if EU legislation establishes more specific rules on environmental claims for a particular sector or product category, such as the 'EU Ecolabel' (the official EU label for environmentally friendly products), or the EU energy efficiency label, those rules will prevail over those of the proposed directive.

Under the proposal, claims are perceived as sufficiently explicit if they are in writing or contained in an environmental label, brand names, company names or product names. An example of claims covered by the proposal could be "packaging made of 30% recycled plastics", or a "commitment to reduce CO₂-emissions linked to the production of this product by 50% by 2030 as compared to 2020".

The Green Claims Directive includes criteria stipulating that environmental assertions must be accompanied by detailed information about the business (e.g., via a QR code per Article 5). Simultaneously,

“ The Green Transition Directive aims to enhance the transparency and reliability of product labelling by prohibiting the utilisation of general environmental claims.

the business is required to conduct a self-assessment to substantiate and certify the environmental claims used. The proposal outlines specific requirements for such an assessment, while Article 11 anticipates the establishment of a verification or certification process in member states. This process involves the independent and publicly accredited third-party verification of businesses' self-assessments and documentation.

SANCTIONS

Should the proposed Green Claims Directive be adopted in its current iteration, member states will be compelled to implement national regulations specifying robust sanctions for infringements of the "green claims" rules, encompassing both incentives and penalties as regulatory instruments. Legitimate environmental claims will be rewarded, while deceptive or incomplete environmental claims will face stringent sanctions.

Article 13 of the Green Claims Directive, read in conjunction with Article 17, mandates that sanctions should be proportionate and reasonably related to the infringements, including fines that effectively deprive the wrongdoer of the economic benefits derived from the violation. These penalties may encompass measures such as the confiscation of proceeds from products falsely marketed as environmentally friendly, temporary exclusion from public procurement procedures, and denial of access to public financing.

Contacts



Elise Johansen
Partner
elj@wr.no



Tonje H. Geiran
Specialist Counsel
tog@wr.no



EU agreement on corporate due diligence rules to safeguard human rights and environment

On 14 December 2023, the European Parliament and the European Council informally agreed on a new directive on corporate sustainability due diligence (the “CS3D” or the “directive”) obliging firms to integrate their human rights and environmental impact into their management systems. The directive has been called a historic breakthrough in the way companies are now responsible for potential abuse in their value chain. Subsequent to the negotiations, the lead MEP said that this was a starting point for shaping the economy of the future.

The new directive, building on the proposal from the Commission of 23 February 2022 ([see our previous newsletter here](#)), follows in the wake of consistent [calls from the European Parliament](#) for a wider reaching corporate accountability and mandatory due diligence legislation. Indeed, in the aftermath of the negotiations, [the lead MEP said](#) that this was a starting point for shaping the economy of the future; “one that puts the well-being of people and the planet before profits and short termism”. The CS3D must also be understood in a broader context, as it complements existing and upcoming legislative acts, such as the deforestation regulation, ([EU/2023/1115](#)) the conflict minerals regulation, ([EU/2017/821](#)) and the draft regulation prohibiting products made with forced labour. [For a more detailed description of this, see e.g here](#). The CS3D is also intricately linked to the Corporate Sustainability Reporting Directive (CSRD). While the CS3D mandates companies to assume environmental and social responsibilities, the CSRD mandates transparency for European companies regarding these responsibilities.

The agreed draft law requires formal approval by the Legal Affairs Committee and the European Parliament as a whole, in addition to the Council, before it can enter into force. In practice however, significant material changes are less common at this later stage, and there are therefore good reasons to pay close attention to the scope and content of the draft CS3D even now.

In essence, the provisional agreement outlines the scope of the directive, elucidates the responsibilities of non-compliant companies, provides clearer definitions for various penalties, and supplements the list of rights and prohibitions that companies are expected to adhere

to. However, the text of the CS3D is not yet published (as of medio January 2024), and there are certain discrepancies in the sources relating to the precise content and applicability of the CS3D. Once the final text is published, we will have further clarity on scope and key content, as well as sanctions, responsibility and supervision. Below is an overview of these key areas as can currently be gleaned from various official EU sources (e.g. [Corporate due diligence rules agreed to safeguard human rights and environment \(europa.eu\)](#) and [Corporate sustainability due diligence: Council and Parliament strike deal to protect environment and human rights - Consilium \(europa.eu\)](#)).



Companies will have to identify, assess, prevent, mitigate, bring to an end and remedy their negative impact on human rights and the environment.



Companies that already conduct human rights due diligence in line with the Norwegian Transparency Act will be well positioned to meet the requirements under the new directive, although differences in scope will likely require an expanded due diligence focus.

SCOPE

As proposed, the directive will apply to EU and non-EU companies of a considerable size and economic heft.

1. Firstly, the legislation will apply to EU companies, and their parent companies, with a workforce exceeding 500 employees and a global turnover in excess of 150 million euros.
2. Second, the legislation will apply to EU companies and their parent companies, that have at least 250 employees and a turnover exceeding 40 million euros, provided that a minimum of 20 million euros is generated within a “high impact sector” – as closer outlined in the directive. Examples of such sectors include agriculture, fisheries, extraction of mineral resources, construction and textiles.
3. Furthermore, the legislation will apply to non-EU companies with a turnover in the EU exceeding certain thresholds. There are some discrepancies in the relevant press releases regarding the applicable thresholds, varying from an EU turnover of 150 to 300 million euros.

A controversial topic worth noting is that the compromise agreement reportedly excludes the core business of financial actors, namely their investment and lending activities, from the scope of the directive. Nevertheless, a review clause has allegedly been incorporated to as-

sess the potential inclusion of the financial downstream sector in the future, contingent upon a sufficient impact assessment.

KEY CONTENT

The CS3D contains two key obligations.

First, the new directive sets out obligations for in-scope companies to integrate a due diligence regime into their policies and risk management systems. Companies will have to identify, assess, prevent, mitigate, bring to an end and remedy their negative impact on human rights and the environment, and that of their upstream business partners and for downstream activities such as distribution or recycling.

Reportedly, the proposal includes a list of certain rights and prohibitions which would constitute adverse human rights impacts if abused or violated. The list makes reference to relevant international instruments that have been ratified by the EU member states, that will help to clarify the obligations by referring to internationally recognised standards.

The CS3D also elucidates the scope of environmental impacts. The definition in the proposal includes any measurable environmental degradation, such as harmful soil change, water or air pollution, damaging emissions, excessive water consumption or other harmful impacts on natural resources. Similar to human rights, adverse environmental impacts are considered to arise from the infringement of specific enumerated rights and prohibitions.

Second, companies of a substantial size and economic heft (i.e. meeting threshold (1) above) will have to adopt a plan to ensure that their business models align with the goal of restricting global warming to 1.5°C.

SANCTIONS, RESPONSIBILITY AND SUPERVISION

Upon implementation, the due diligence obligations will be enforceable primarily through two distinct mechanisms.

- **Civil claims and enforcement orders:** Non-compliant companies can be met with civil liability, as the CS3D establishes a five-year timeframe where those who are affected by an adverse impact can file compensation claims for damages. Furthermore, companies can as a last resort be obliged to terminate business relationships when a given identified adverse impact cannot be prevented or rectified in any other way.
- **Penalties:** Every EU member state will have to appoint a supervisory authority responsible for overseeing companies’ adherence to these obligations. Such entities will have the authority to initiate inspections and investigations, as well as to levy penalties on non-compliant companies. These penalties can for example consist of public exposure (“naming and

shaming”) and/or fines amounting to a maximum of 5% of the global net turnover in the company.

It is also worth noting that the proposal establishes that compliance with due diligence obligations could be considered as a component in criteria used for awarding public and concession contracts. Hence, the proposal also stimulates compliance through positive and financial incentives.

HOW WILL YOUR BUSINESS BE AFFECTED?

The directive is likely to be adopted during the course of 2024. The CS3D will then have to be transposed into national law by the various member states before companies are required to abide by it. The proposed directive has been marked as EEA relevant, and in Norway, alignments with the Transparency Act will likely be required before the directive is implemented into Norwegian law.

Companies that have already conducted human rights due diligence in line with the Norwegian Transparency Act and the OECD Guidelines for Multinational Enterprises will be well positioned to meet the requirements under the CS3D relating to human rights. However, there are differences in scope, for example relating to downstream activities, which means that companies will likely have to expand their due diligence focus.

Another significant distinction, in comparison to the Transparency Act, lies in the incorporation of environmental concerns. Specifically companies will be required to acquaint themselves with the environmental regulations and constraints outlined in the CS3D, thereby expanding the scope of due diligence exercises to encompass these aspects as well.

Addendum: The European Union released the final draft of the CS3D on 30 January 2024. The Council of the European Union will vote on the final text of the CS3D on 9 February 2023.

Sign up for our ESG Alerts

The legal framework in this area of law is expanding significantly, and becoming increasingly complex to navigate. In our ESG Alerts we provide an update covering key developments on topics of relevance under the ESG umbrella. For any questions regarding the current framework or the proposed changes, and how they may affect your business, our team of ESG and compliance experts is always ready to assist.

Contacts



Kristin N. Brattli
Partner
knh@wr.no



Elise Johansen
Partner
elj@wr.no



Hanne R. Gundersrud
Senior Lawyer
hgu@wr.no



Proposed changes to Norway's foreign investment control regime

In December 2023 the Investment Control Commission – appointed by the Norwegian government in 2022 – delivered its report concerning Norway's foreign direct investment (“FDI”) laws. The report proposes significant changes to the current system, ostensibly in order to protect national security interests, and would bring Norway's rules on FDI more in line with some of its European neighbours.



The current provisions governing ownership control, and thereby FDI, are found in the Security Act of 2019. The Security Act is in many ways limited in scope, and there are in practice very few instances where investments in Norwegian companies are subject to regulatory scrutiny by the authorities.

Some changes to the Security Act came into force during 2023, with some further amendments pending, which have incrementally sought to bring Norway's FDI regime up to international standards. However the Investment Control Commission's proposal is, in many respects, to totally overhaul the system and significantly expand the regime. It is estimated that as many as 300 transactions would be subject to mandatory screening each year if the proposed regime were implemented.

INVESTMENT CONTROL TO PROTECT NATIONAL SECURITY INTERESTS

The government appointed the Investment Control Commission to assess whether Norway has a sufficiently robust legal framework in place to handle the risks that may result from foreign investment in Norwegian enterprises. The Commission presented its report in early December 2023.

According to the Commission, the proposed changes are intended to address what they see as significant challenges with the current

investment control regime, in particular that the system is too narrow and fragmented, entailing that relevant investments are not detected systematically or to a sufficient extent. The Commission underlines the need to increase transparency regarding which investments may be subject to screening, to establish suitable legal bases for intervening against proposed investments, and to provide for the uniform processing of cases in a manner consistent with international principles.

THE PROPOSED LEGAL FRAMEWORK

The Commission's main proposals can be summarised as follows:

- A new legal framework for investment control should be developed through specific legislation and appurtenant regulations.
- There should be a single authority responsible for screening investment control cases.
- An obligation to notify certain FDI in "sensitive sectors" should be established. Sensitive sectors include suppliers of important infrastructure, companies producing or controlling critical technology, and companies producing or controlling certain raw materials. However, media companies or companies processing large amounts of personal information or personal data, or real estate, are not included in the proposal.
- The obligation to notify should arise where there is an acquisition of shares or voting rights in a company (falling under the legislation) exceeding ten percent, a third, or two-thirds. Investors should however be able to increase their ownership within each



The Investment Control Commission's proposal is, in many respects, to totally overhaul the system.

interval without triggering a new notification obligation. However, upon exceeding a new interval, renotification may be required.

- A distinction should be made between EEA-based investors and “third country” investors. While there would be a notification obligation on all investors in certain sensitive sectors, other obligations would only be placed on investors from third countries.
- A voluntary notification regime should be introduced, applying to all sectors, where the investment is not covered by an obligation to notify but may still constitute a security risk.
- For notifications, there should be an initial timeline of 25 working days for the authority to assess whether the investment can be approved. If the investment is not approved within 25 working days, the authority can look at the case in further detail but its assessment should not, in general, exceed 90 working days from when the notification was submitted.
- The authority should have the power to (i) make its approval conditional on certain steps being taken, and (ii) prohibit or annul an investment if it poses a not insignificant threat to national security interests.
- Fixed criteria for how the authority should assess cases should be developed.

ALIGNING THE REGIME WITH INTERNATIONAL STANDARDS?

Norway is trailing its Nordic and European neighbours when it comes to regulating FDI. Sweden’s new legal framework came into force on 1 December 2023, completely overhauling Sweden’s approach to FDI. Denmark introduced new rules already in 2021.

Implementing the proposals from the Commission would bring Norway closer to the prevailing European standard for FDI control. However, it remains unclear whether there is sufficient political will to implement a total reform of the system at this stage. Several amendments to the Security Act came into force only earlier this year, and further changes are yet to be implemented. There may be some desire to see how these changes play out before enacting a further overhaul.

However, if there is a will to make further, more far reaching, changes, implementing the proposals of the Commission would provide more legal certainty for investors and – critically – more transparency over how cases should be dealt with. That, in itself, should be sufficient reason to consider supporting these proposals, and we look forward to the public consultation process that will follow the Commission’s work.

For any questions regarding the current framework or the proposed changes and how they may affect your business, our team of FDI experts is ready to assist.

Contacts



Stuart Stock
Specialist Counsel
sts@wr.no



Patrick Oware
Senior Associate
pkowr@wr.no

Two years following the invasion of Ukraine – some lessons learnt

The massive and unprecedented sanctions imposed against Russia have required significant efforts to manage the risks and impact of sanctions, particularly in view of creative attempts to circumvent by some parties. In this article we explain why you should update your sanctions clause, and how to ensure that it is fit for purpose.

Sanctions have been imposed against Russia since the invasion of Crimea in 2014. However, the full-scale invasion of Ukraine in February 2022 has led to unprecedented sanctions being imposed by various authorities, not only in those jurisdictions most commonly associated with setting the agenda on sanctions. Tools never used before are now being applied for the first time. International trade is becoming increasingly difficult and cumbersome, particularly in areas such as energy, transport and commodities.

Violations of sanctions can lead to a wide array of adverse consequences, including civil and in some cases criminal liability: vessels being sanctioned, seized or delayed, or termination of credit facilities or key services such as insurance. The list of trading restrictions seems ever expanding. Needless to say, many operators have a rather low risk appetite when it comes to sanctions, but on the other hand, losing key business streams or ending up in legal disputes by adopting an unnecessarily restrictive approach is also undesirable.

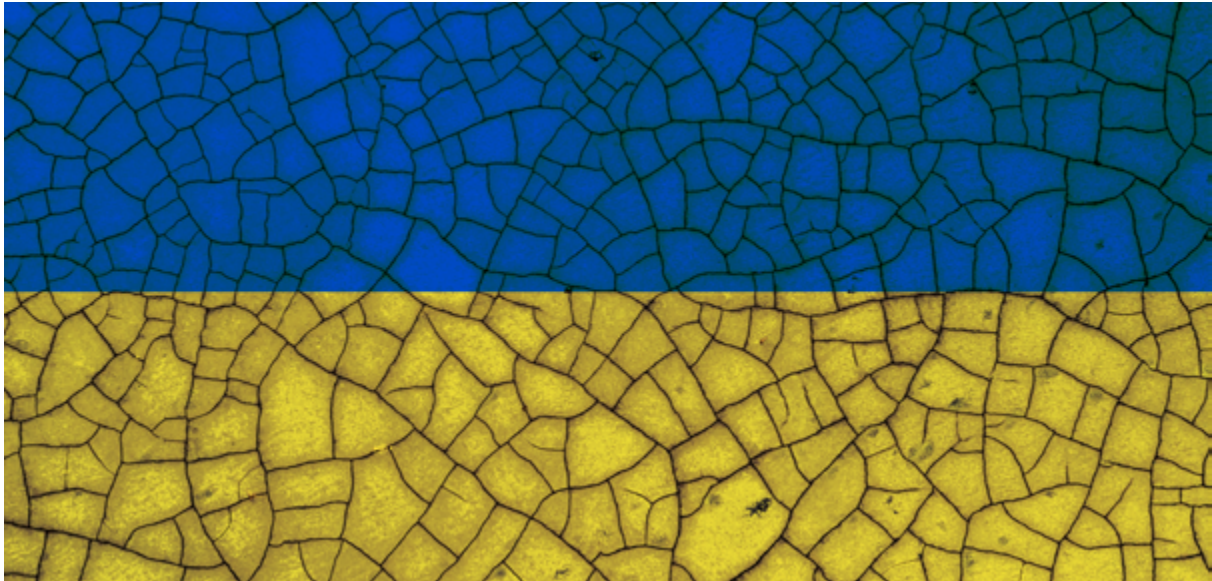
RISK-BASED TRIGGERS ARE PREFERABLE

Sanctions clauses are essentially specialised ‘change of circumstances’ clauses, in the same family as force majeure, hardship, change in laws, and price revision clauses. Their purpose is to provide a framework for the parties to respond to certain events. As such, they tend to have two main components – a trigger telling you when the clause applies, and an operative part providing for the consequences, usually suspension and/or termination of the contract, but more nuanced provisions can also be used in certain cases.

The trigger will typically include a list of events, such as the designation of a party or its owner on a sanctions list, and/or a more general provision trigger-



A good contractual solution, particularly for longer-term contracts or those that may be exposed to geopolitical risk, is a risk-based trigger.



ing the clause if performance of the contract would lead to a breach of sanctions (for example, the import of a prohibited commodity). The latter provision, i.e., sanctions events which do not amount to designation of a party, can be particularly important. Sanctions do not always fit into pre-defined categories, and in our experience a carefully worded trigger provision can be invaluable to avoid disputes.

In a dispute, a court or tribunal will start by analysing the applicable sanctions laws and jurisdiction, and then make a decision as to whether the clause applies to the relevant factual matrix (or if there is an ‘at law’ rule to follow), based on the preponderance of the evidence available. These cases frequently present evidential difficulties. For example, it may not be possible to establish whether one person should be ‘deemed’ to control another for sanctions purposes, because such an arrangement will likely have been put in place secretly and with a view to circumvention (as we note below). More generally, it can be difficult to obtain materials from certain closed corporate registries to evidence ownership, or it may be necessary to seek expert guidance as to whether certain products fall within the scope of what is prohibited under trading restrictions.

In simplified terms, the court or tribunal will assess whether it is more likely

than not that a trigger event took place, and the natural interpretation of the clause governing the parties’ response to that trigger. If it is found that the relevant activity does not breach sanctions, or there is an appropriate contractual remedy that ought to have been adopted, then a terminating or suspending party may themselves be at risk of being in breach of contract. Our experience is that most corporations would rather risk a breach of contract than a violation of sanctions if forced to make a choice in this respect, given the potential severity of the consequences of a sanctions violation.

A good contractual solution, particularly for longer-term contracts or those that may be exposed to geopolitical risk, is a risk-based trigger, rather than a trigger requiring an actual sanctions violation. In our experience, proving that performance of an activity “exposes” a party to “risk of sanctions violation” or even “may/could” breach sanctions, is significantly simpler than proving that performance actually breaches sanctions. It would in such cases usually be reasonable to act based on an independent legal opinion indicating the relevant risk, even if the position is not wholly certain.

DESIGNATIONS

Many of the sanctions directed against the Russian Federation after the full-scale

invasion of Ukraine have targeted wealthy individuals said to be close to and/or to have benefitted from President Putin's kleptocratic regime, also known as oligarchs. The US Treasury Department in 2018 published a list of 114 senior political figures close to Putin and 96 oligarchs with a net worth of USD 1 billion or more. Many of these oligarchs have been sanctioned by various authorities since February 2022 or earlier.

Sanctions against oligarchs typically take the form of asset freezes, which in respect of EU and UK sanctions means that all funds and economic resources belonging to, owned, controlled or held by the designated individuals (directly or indirectly) must be frozen. Further, no benefit should be provided to designated individuals, directly or indirectly. These provisions are drafted and interpreted widely. This effectively prohibits trade with both the designated individual, and any companies which they control or have majority ownership in.

US sanctions rather clinically focus on ownership under the so-called "OFAC 50%

rule". Under EU and UK legislation it is also relevant whether the individual may be deemed to control the relevant entity, a test which is highly fact based and can potentially apply in cases with minority ownership by the designated individual. In the UK, we must also consider if there are reasonable grounds to suspect that a party is owned or controlled by a designated individual, which adds an additional layer of subjectivity to an already complex assessment.

A typical response by companies which have designated individuals as managers or shareholders, is to have the designated individuals resign from relevant positions, and divest themselves of their direct or indirect shareholding positions (to below 50%). While this is done legitimately in some cases, these arrangements can involve attempts to disguise continuing control, for example by (i) ownership through trusts or frontmen, (ii) ownership located in jurisdictions with limited transparency as regards beneficial ownership, and/or (iii) unknown or circular ownership. These have been a rather common method since oligarchs first became targets of US and EU sanctions after Russia's 2014 invasion of Crimea.

For the counterparty, the challenge is that control may be exercised through other mechanisms than management positions and ownership. New managers and owners may have informal links to the sanctioned individuals, and the new owners' finance arrangements may ultimately leave control with the former owner. As with the sanctions clause trigger, the counterparty may end up in an evidentiary dilemma. It is in our experience very difficult to prove your suspicions of hidden means of control. While it may be possible, it will often involve a very deep dive into publicly available sources and require

Sign up for our Sanctions Alerts

Sanctions and trade compliance is becoming increasingly complex to navigate. WR Sanctions Alerts provide you with updates on material developments in the country-specific sanctions programmes implemented by the US, the UN, the UK, the EU and Norway.

assistance from local investigators and experts. On the other hand, sanctions authorities (such as the UK) may require you to suspend trade if you have cause to suspect that the sanctioned individual remains in control.

CHANGE OF CONTROL

For parties who need to manage the risk of future designations within their counterparty (starting from an assumption that the trade and counterparty is presently not sanctioned), one solution is a 'change of control' provision within the sanctions clause. It may also be helpful to add such provisions elsewhere, including with respect to credit support providers or other entities expected to perform activities under the contract. Change of control clauses are common in contracts where the ownership and/or control of your counterparty is essential, and allow a party to terminate the contract in case of a change in control of the other party. (Corporate lawyers will recall searching for such clauses in due diligence with some trepidation!).

In a sanctions clause, the change of control can work in two ways. Firstly, it can be used within a sanctions clause to solve the above evidentiary dilemma – where there is any divestment or change in ownership reported, that can be relied on – rather than seeking to ascertain the full facts of the new ownership or any subjective control issues. This enables termination or suspension based solely on the purported divestment. Secondly, an analogous provision can be used to enable termination or suspension unless there is a change in control, change in management or novation of the contract. That may be appropriate where there is a crucial long-term supply to be maintained, which can lawfully be continued if the involvement of designated persons is removed. There

are still risks in this scenario that would need to be considered on a case by case basis, i.e., there may be apparent compliance with the designated person retaining informal control.

WHAT ELSE?

In any consideration of a sanctions clause or of general sanctions risk, it is necessary to consider whether a general clause is sufficient, or whether a more bespoke provision needs to be put in place. Particular industries will also carry their own particular risks (and in some cases have their own standards to work from). For example, industries which involve multiple deal participants or which may operate in more opaque jurisdictions (such as shipping, offshore drilling, and international trade), will usually require greater due diligence. It can be helpful in such cases to place a higher burden on the counterparty in terms of representations and warranties as to their own compliance/reporting, and not rely solely on a trigger becoming apparent.

In addition to updating your sanctions clause, you may want to use the momentum to update your sanctions compliance programme. A fundamental element in this regard is to conduct a sanctions risk assessment that considers the specific risks of your business, including clients, products, services and geographic locations. Mapping and assessing risks – also looking forward – may be particularly useful now in light of the tense geopolitical situation, not only due to Russia's war, but also tensions in China and the Middle East.

Our sanctions team can help with practical compliance programmes, drafting effective sanctions clauses, and managing sanctions disputes. Please get in touch if you would like further information or assistance.

Contacts



Aadne M. Haga
Partner
aha@wr.no



Elisabeth Roscher
Partner
elr@wr.no



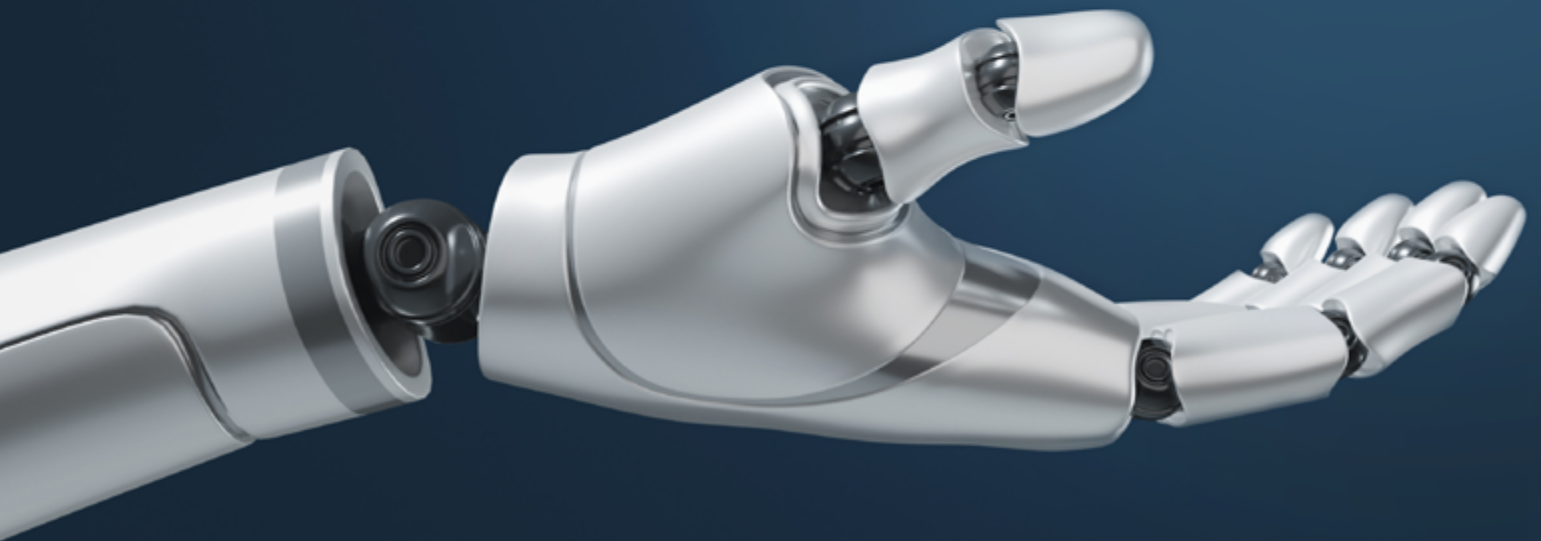
Tine E. Vigmostad
Partner
tvi@wr.no



Eleanor Midwinter
Consultant

Towards safe, reliable and human-centred AI

The EU's Artificial Intelligence (AI) Act marks a global first, introducing rules for the use and provision of AI systems. At the heart is a commitment to fostering trust in AI to unlock and maximise the vast social and economic possibilities offered by these technologies.





Europe is closer than ever to having the world's first comprehensive legal framework in artificial intelligence. [A draft final text on the AI Act was leaked on 22 January 2024](#) – a month and a half after the European Council and Parliament announced that they had reached political agreement on the rules. In this article, we touch upon the legislative status of the AI Act and its key elements.

LEGISLATIVE STATUS OF THE AI ACT

The AI Act was proposed by the European Commission in April 2021. On 2 February 2024, the European Council, through the Permanent Representative Committee (COREPER), consisting of member states' representatives, adopted the final text.

[The European Parliament is expected to undertake a first vote in committees in mid-February](#), followed by plenary votes in March or April.

If both the Council and the Parliament confirm the final text, the AI Act will be published in the Official Journal of the European Union and enter into force on the twentieth day following its publication. This is expected to happen before the summer. [The Act will apply in the EU two years after its entry into force](#), with specific application dates for different provisions ranging from six months to 36 months following the entry into force.

The Act has been indicated by Norwegian government representatives as EEA relevant. Therefore, businesses in Norway providing, using, importing or distributing AI systems should familiarise themselves with the regulations under the AI Act and prepare for compliance.



Businesses in Norway providing, using, importing or distributing AI systems should familiarise themselves with the regulations under the AI Act and prepare for compliance.

Our Technology and Digitalisation team is following the legislative developments closely and will be happy to answer your questions.

KEY ELEMENTS OF THE AI ACT

Scope and application

The Act applies primarily to **providers** of AI systems (whether established in the EU or not), **deployers** of AI systems within the EU (or systems whose output is used in the EU), **importers** and **distributors** of AI systems and **product manufacturers** which place on the market or put into service an AI system together with their product.

There are certain exemptions in the AI Act for use of AI systems for military, defence or national security purposes, law enforcement, judicial cooperation and scientific research and development purposes.

Moreover, the Regulation shall not apply to AI systems which are under development and AI systems released

under free and open source licences (with certain exceptions for high-risk AI systems and systems which are tested in real world conditions). AI systems which are used by natural persons in the course of a purely personal, non-professional activity are also exempt from the scope of the AI Act. The majority of the provisions in the AI Act are aimed at prohibiting certain AI systems and regulating high-risk AI systems. There are no obligations relating to lower-risk AI systems, such as simple chat bots, other than simple transparency obligations in some cases.

Prohibited AI systems

The AI Act prohibits the provision and use of AI systems which:

- deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques;
- exploit vulnerabilities of individuals or specific groups of persons due to their age, disability or a specific social or economic situation;
- categorise individuals based on their biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation;
- evaluate or classify individuals or groups over a certain period of time based on their social behaviour or personal characteristics (social scoring);
- use biometrics to remotely identify individuals in 'real-time' in public spaces for law enforcement purposes unless strictly necessary for specified purposes (targeted victims search, threat prevention, localisation, identification or prosecution of suspects of certain criminal offences);
- are used for predictive policing, based solely on the profiling of individuals or on assessing their personality traits and characteristics;



The Act applies primarily to providers, deployers, importers and distributors of AI systems as well as product manufacturers which place on the market or put into service an AI system together with their product.

- create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; and
- are used to infer individuals' emotions in the workplace or educational institutions.

High-risk AI systems

While the above AI systems are prohibited, high-risk AI systems are allowed if certain criteria are fulfilled. Examples of high-risk AI systems are systems used:

- as a safety component in products or which are products subject to legislation specified in Annex II of the Act (relating e.g. to machinery, toys, radio equipment, medical devices, civil aviation, marine equipment, rail interoperability, or motor vehicles);
- with biometrics for remote biometric identification, biometric categorisation or emotion recognition;
- as safety components to manage and operate critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity;
- in the educational sector to determine access or admission, evaluate learning outcomes, assess the appropriate level of education for individuals or monitor and detect prohibited behaviour of students;
- in the context of employment, to recruit individuals, make decisions affecting employees' work terms, allocate tasks or monitor and evaluate employees' performance;
- to evaluate individuals' eligibility for essential public assistance benefits and services or grant, and reduce, revoke or reclaim them;
- to evaluate individuals' creditworthiness/score;
- to evaluate and classify emergency calls or to prioritise dispatch;
- to assess individual risk and pricing for life and health insurance;
- in law enforcement to assess the risk of individuals becoming victims or offenders, as support polygraphs and similar tools, to evaluate the reliability of evidence, or to profile individuals;
- by immigration authorities as support polygraphs and similar tools, to assess specific risks posed by individuals, examine immigration applications and the reliability of evidence, or detect, recognise or identify individuals;
- by judicial authorities to research and interpret facts and the law;
- to influence the outcome of an election or referendum, or the voting behaviour of individuals.

Obligations relating to high-risk AI systems

The main requirements for **providers** of high-risk AI systems are as follows:

- establish, implement and document a risk management system;

- only use data which meet certain quality criteria in training, validation or testing;
- draw up technical documentation before the high-risk system is placed on the market or put into service;
- ensure that systems have capability for the automatic recording of events (logging);
- ensure that systems' operation is sufficiently transparent to enable deployers to interpret the output and use it appropriately;
- ensure that systems can be effectively overseen by natural persons;
- design and develop systems in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity;

The main requirements for **deployers** (i.e. professional users) of high-risk AI systems are as follows:

- take appropriate technical and organisational measures to ensure appropriate use of the system;
- assign human oversight;
- ensure input data is relevant and sufficiently representative in view of the intended purpose of the system;
- monitor the operation of the system and immediately inform first the provider, and then the importer or distributor and relevant authorities if they have identified any serious incident;
- keep the logs automatically generated by that system to the extent such logs are under their control for a period appropriate to the intended purpose of the system, of at least six months;
- perform Data Protection Impact Assessments (DPIAs) to the extent required under the GDPR;
- where the deployer is a public body or private body operating public services, or where the deployer uses AI systems for credit scoring or to perform risk assessment and pricing towards individuals seeking health or life insurance, perform fundamental rights impact assessments; and

- where the deployer is an employer implementing an AI system in the workplace, inform the affected workers.

Importers and distributors shall verify that the provider has complied with its obligations under the AI Act before placing a high-risk AI system on the market. Importers and distributors are also subject to additional obligations which are described in Article 26 and Article 27 of the Act respectively.

Providers of **General Purpose AI systems (GPAI)** and **certain other AI systems** are subject to additional transparency obligations, such as the following:

- ensuring that AI systems intended to directly interact with individuals are designed and developed to inform individuals that they are interacting with an AI system;
- deployers of emotion recognition systems or biometric categorisation systems shall inform affected individuals about their operation;
- providers of AI systems (including GPAI) generating synthetic audio, image, video or text content, shall ensure the marking of outputs as artificially generated or manipulated; and
- deployers of AI systems that generate or manipulate image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated.

There is a separate Chapter under the AI Act for GPAI systems, regulating classification of these systems and obligations for providers of GPAI models.

Consequences of non-compliance

Non-compliance with the provisions under the AI Act might lead to fines up to EUR 35 million or up to 7% of a company's total worldwide annual turnover for the preceding financial year, whichever is higher.

Contacts



Lars Erik Steinkjer
Partner
lst@wr.no



Gry Hvidsten
Partner
ghv@wr.no



Ekin Ince Ersvaer
Paralegal
eie@wr.no

Are all state-owned Russian companies controlled by President Putin?

This was a question many asked after a recent judgment from the English Court of Appeal. Sanctions target those designated as well as those owned or controlled by designated persons. Understanding the precise scope of what constitutes ‘control’ under UK sanctions can be challenging. In this article we shed some light on this analysis, based on recent case law.

In January 2023, the English High Court issued a judgment (*PJSC National Bank Trust and another v Mints and others* [2023] EWHC 118 (COMM) (“**Mints**”)) concerning the conduct of litigation by sanctioned persons, specifically whether the defendants should be granted a stay of proceedings due to the sanctioned status of certain claimants. The key issues were (i) whether the Court could enter judgment on a claim brought by a sanctioned person, or whether the proceedings should be stayed pending lifting of sanctions, and (ii) whether orders for costs, security and damages could be made and satisfied to or by sanctioned persons, and whether such actions were licensable by OFSI. These issues arose because the second claimant, Bank Okritie, was sanctioned by the UK. The Court ruled that no stay was necessary and that, to the extent required, the relevant actions were licensable by OFSI.

An ancillary issue in the case was whether the first claimant, PJSC National Bank Trust, was also sanctioned, by virtue of deemed ‘control’ of that claimant by sanctioned persons, namely Vladimir Putin and Elvira Nabiullina (Governor of

Russia’s Central Bank). The Court ruled that the first claimant should not be deemed as sanctioned. This was, in broad terms, because (i) the control test needed to be viewed through the lens of the primary test of ownership i.e., be something akin to ownership, (ii) it would be unfair for market participants not to be in a position to readily understand if an important company was

to be treated as sanctioned, and (iii) pure political influence, separate from more tangible ownership or control, should not automatically be equated with control. That part of the judgment was *obiter*, which means that it was not determinative of the main issues, and as such did not create a binding precedent.

However, because it concerned points which practitioners and mar-



While recognising that the judgment could lead to the “absurd” outcome that every company in Russia could be deemed to be controlled by Mr Putin and hence sanctioned, the judge commented that the remedy would be for the UK government to amend the law or provide appropriate guidance.

ket participants have been grappling with for some time with limited official guidance, these *obiter* comments attracted significant attention and fed into sanctions advisory work.

As was expected, the defendants appealed. On 6 October 2023, their appeal was rejected by the Court of Appeal ([2023] EWCA Civ 1132). In summary, the Court of Appeal ruled that:

- UK sanctions on Russia do not curtail a designated person's ability to bring civil proceedings or the court's ability to give a money judgment in favour of a designated person, therefore there should be no stay of proceedings; and
- In any event, OFSI can license certain orders, including costs orders and orders for security for costs, both for or against a designated person.

While no decision was technically required on the 'control' issue (due to it being *obiter*) the general importance of the issue was recognised, and as such, it was briefly dealt with by the Court of Appeal. Importantly, this included comments to the effect that:

- PJSC National Bank Trust is "controlled" by President Putin and/or Ms Nabiullina within the meaning of UK sanctions on Russia.
- The first instance judge, Cockerill J, had erred by "*reading in*" wording to the UK sanctions legislation and finding that there was a carve-out from

the control test for control by political office, or in seeking to constrain the ambit of the test on the basis of perceived unfairness. The relevant test in the Russia Regulations 7(4) is extremely wide, using words such as "*in all the circumstances*" and control "*by whatever means*". This broad ambit should be taken as clearly intended by the UK government, given the absence of any carve out.

- Specific reference was made to the fact that Mr Putin is at the "*apex of a command economy*" and that, as such, state ownership is a highly relevant factor when considering control. While recognising that the judgment could lead to the "*absurd*" outcome that every company in Russia could deemed to be controlled by Mr Putin and hence sanctioned, Flaux LJ commented that if this applies, then the remedy is for the UK government to amend the wording of the Russia Regulations or provide appropriate guidance.

The Court of Appeal's judgment highlighted the risks which can arise from hastily implemented legislation. In addition, and whether intentionally or not, the judgment created significant uncertainty for practitioners and UK market participants alike. Indeed, the approach taken by the Court of Appeal to the ownership and control test gave rise to the possibility that all Russian entities must be considered subject to UK sanctions

on the basis that they are controlled by Vladimir Putin. Although, like the first case, this aspect of the judgment was *obiter* and did not create binding precedent, it nonetheless caused a stir among market participants.

POST-MINTS: UK GOVERNMENT APPROACH AND SUBSEQUENT CASE LAW

UK government approach

In light of the uncertainty generated by the *obiter* comments of the Court of Appeal, the Foreign Commonwealth & Development Office (FCDO) released the following statement, in response to the judgment to clarify the UK government's position:

"The Government is carefully considering the impact of the Court of Appeal's judgment in Mints & others v PJSC National Bank Trust & another, in particular the Court's views that PJSC National Bank Trust is 'controlled' by Designated Persons by virtue of their political office, noting that the case was not decided on this point.

FCDO would look to designate a public body where possible when designating a public official if FCDO considered that the relevant official was exercising control over the public body.

There is no presumption on the part of the Government that a private entity based in or incorporated in Russia or any jurisdiction in which a public official is designated is in itself sufficient evidence to demonstrate that the relevant official exercises control over that entity.



In the interests of reducing any uncertainty, we are exploring the options available to the Government in clarifying this position further.”

In addition to this statement, further guidance was issued in order to clarify the “*policy intention of the UK government’s approach to ownership and control in UK sanctions regulations...*”. The key takeaways were as follows:

- The FCDO does not generally consider designated public officials to exercise control over a public body in which they hold a leadership function.
- If the FCDO considered that a public official was exercising control over the public body under UK sanctions regulations, FCDO would look to designate the public body at the same time as designating the relevant public official.
- There is no presumption on the part of the UK government that a private entity is subject to the control of a designated public official simply because that entity is based or incorporated in a jurisdiction in which that official has a leading role in economic policy or decision-making.
- Specifically, for the purposes of regulation 7(4) of the Russia (Sanctions) (EU Exit) Regulations 2019, the UK government does not consider that President Putin exercises indirect or de facto control over all entities in the Russian economy merely by virtue of his occupation of the Russian Presidency.

The guidance helpfully establishes that the UK government does not consider all Russian companies to be deemed designated persons by virtue of Vladimir Putin’s own designation. Although the statement is just guidance and does not have the force of law, it strongly suggests that UK enforcement authorities

would be unlikely to take action against companies for dealing with non-designated private sector Russian persons.

Litasco SA v Der Mond Oil and Gas Africa SA & Locafrique Holdings SA [2023] EWHC 2866 (Comm) (“Litasco”)

In November 2023, the English High Court handed down the first binding decision relating to the “control” issue in the case of *Litasco*. The case concerned the failure of the Respondent (Der Mond) to fulfil certain payment obligations relating to trades of Nigerian crude oil. As part of its defence, the respondent proffered, amongst other arguments, that the claimant (*Litasco*) and its parent company, Lukoil, were controlled by Vladimir Putin and therefore subject to UK sanctions. The respondent relied upon the discussion of this issue in *Mints* to further its argument.

Dismissing the argument, Foxton J sought to distinguish the facts in *Litasco* from those in *Mints*, as a means of dealing with the comments made by Flaux LJ and the Court of Appeal. Indeed, it was noted by Foxton J that it was not surprising that PJSC National Bank Trust was deemed as being controlled by Vladimir Putin on the basis that it was “*an organ of the state over which President Putin exercised de facto control*”. Conversely, Foxton J concluded that, with respect to *Litasco*, there was no evidence to show (or arguably show) that *Litasco* was presently under the de facto control of Vladimir Putin. This was because *Litasco*’s parent company, Lukoil, was a private company and clearly not an arm of the Russian state.

CONCLUSION

The crux of *Litasco*, and what practitioners and UK market participants should take into account when assessing control, is that “*an existing influence*” by a sanctioned person over the relevant business of a company is required (i.e. *de facto*

control). The fact that a sanctioned person could, in theory, influence the operations of a company is insufficient for the purposes of the control test. Indeed, Foxton J commented that with respect to *Litasco*, Vladimir Putin was “*wholly ignorant*” of *Litasco*’s existence and *Litasco*’s affairs “*were conducted on a routine basis without any thought of him*”.

The conclusions reached by Foxton J on the control test are thus more aligned with the UK government guidance and go at least some way to alleviating the concerns caused by the *obiter* comments of Flaux LJ in *Mints*.

Nonetheless, market participants and practitioners must still conduct sufficient due diligence to assess whether a counterparty may be subject to *de facto* control (“*existing influence*”) by a designated person. In particular, where sanctions “red flags” are present, market participants should engage in a robust due diligence process. In this regard, OFSI has laid out steps in its enforcement guidance at paragraphs 3.23 – 3.32, with particular reference to ownership and control, that may assist.

The Wikborg Rein sanctions team is also on hand to answer any questions or provide assistance on all aspects of counterparty due diligence.

Contacts



Tine E. Vigmostad
Partner
tvi@wr.no



Hanne R. Gundersrud
Senior Lawyer
hgu@wr.no



Jack Wray
Associate
jwr@wrco.co.uk



What practitioners and UK market participants should take into account when assessing control, is that “an existing influence” by a sanctioned person over the relevant business of a company is required.



A photograph of the Shanghai skyline at dusk, featuring prominent skyscrapers like the Shanghai Tower and the Oriental Pearl Tower. The buildings are silhouetted against a clear blue sky, with some lights beginning to glow. In the foreground, a paved promenade with a metal railing and two street lamps is visible, overlooking the water.

How to navigate China's anti-sanctions laws amidst the sanctions against Russia

Chinese countermeasures may get renewed relevance for foreign companies with operations in China or doing business with Chinese counterparties as a result of the sweeping sanctions implemented against Russia. Companies should tread carefully to avoid falling foul of Chinese legislation.



Over the past few years, China has enacted a suite of laws and regulations aimed at protecting the interests of Chinese individuals and organisations, particularly from the effect of restrictions in non-Chinese legislation. The most applicable law within this framework is the “**Countering Foreign Sanctions Law**” (often referred to as the “**Anti-Sanctions Law**”) which came into force on 10 June 2021.

The Anti-Sanctions Law builds upon other recent regulations, such as the “**Rules on Counteracting Unjustified Extra-Territorial Application of Foreign Legislation and Other Measures**” (the “**Rules**”) issued on 9 January 2021. The Rules apply to situations where the extra-territorial application of non-Chinese legislation hinders Chinese individuals and organisations in their dealings with a person or organisation from a third state. The Anti-Sanctions Law targets restrictive measures against Chinese entities more broadly and expands the toolkit available to Chinese authorities to implement countermeasures.

THE ANTI-SANCTIONS LAW – AN OVERVIEW

While purported to be a defensive measure – similar in some ways to regulations such as the EU Blocking Statutes – the Anti-Sanctions Law goes beyond a mere blocking statute prohibiting compliance with certain foreign sanctions. Rather, the Anti-Sanctions Law introduces two principal protective measures by granting the relevant government department the authority to:

- establish and conduct countermeasures corresponding to the discriminatory restrictive measures; and
- issue a counter-list of individuals or organisations, and certain related parties such as an individual’s spouse or a company’s senior managers, involved in the implementation of such measures (the “**Counter List**”).

Measures, including prohibition of entry and exit, confiscation and freezing of assets in China, and prohibition of transactions and other activities by the listed individual or organisation, may also be implemented against anyone put on the Counter List.

In addition to the countermeasures that may be implemented by governmental authorities, the Anti-Sanctions Law gives Chinese individuals and organisations a legal basis for action against any organisation or individual that assists in the implementation of discriminatory restrictive measures against them. The available remedy is to request an order to stop the infringement and claim compensation for any losses. Chinese law does not normally contain a right to compensation for indirect and/or consequential loss, meaning the Anti-Sanctions Law, on its wording, suggests a wider scope for claims of loss than other Chinese laws.

In the context of sanctions against Russia and Russian entities, the ap-



The Anti-Sanctions Law targets restrictive measures against Chinese entities more broadly and expands the toolkit available to Chinese authorities to implement countermeasures.

plication of the Anti-Sanctions Law in situations where sanctions against Russia have an indirect effect on Chinese individuals and organisations, is not yet settled law. At the time of writing, China has updated the Counter List in December 2022 and April 2023, but only in response to measures by the US against China. However, it should be noted that the Anti-Sanctions Law is broadly worded and that we have yet to see any relevant enforcement or judicial interpretation under it. We therefore recommend keeping a close eye on the Chinese government's further enforcement or judicial interpretation of the Anti-Sanctions Law.

NEW AND EXISTING CONTRACTS

In many jurisdictions, including China, Norway, and England, a contractual basis is needed to terminate the contract or suspend performance due to sanctions. Absent a sufficiently robust sanctions clause, termination may, therefore, be a breach of contract that gives the counterparty a right to claim damages.

Notwithstanding the position under the relevant governing law, a party exercising a right under a sanctions clause that has been negotiated and agreed to by the parties is also less likely to be deemed to be implementing discriminatory restrictive measures under the Anti-Sanctions Law (although such acts can still be considered to breach the law). Therefore, it is usually prudent to include sanctions clauses where relevant in new contracts.

OTHER RELEVANT CHINESE REGULATIONS

While it is less likely that a breach of contract due to sanctions compliance would constitute a breach of Chinese administrative or criminal law, companies operating in China should be aware that other types of regulations may be relevant.

For new projects, the Chinese Anti-Monopoly Law may come into play if the foreign company abiding by sanctions is regarded as an operator holding a dominant market position. Refusing to transact with relevant counterparties without justified reasons may be regarded as abusing a dominant market position. Notably, what is considered a justified reason under the Anti-Monopoly Law is subject to the discretion of the relevant local authority.

Needless to say, if the Chinese government does not support Western sanctions, abiding by them might not constitute a "justified reason". A company abusing its dominant market position, may be ordered to cease its illegal activities, have any illegal earnings confiscated, and/or be fined between 1% to 10% of the previous year's sales revenue.

BEST COURSE OF ACTION

It is worth keeping in mind that, although performance of a contract may currently be illegal under applicable sanctions, even a sanctioned party is not stripped of their legal rights under a contract. For example, a sanctioned party may still bring a claim for wrongful termination, even years from now, leaving companies exposed to legal liabilities if and when the relevant sanctions are lifted.

Importantly, not all sanctions will require suspension of performance. Debt prohibitions, for example, may in certain cases instead be handled through renegotiation of payment terms. Companies should therefore carefully review existing contracts and applicable sanctions before deciding on the best course of action.

Wikborg Rein's international lawyers, including our lawyers in Shanghai, are well placed to help companies navigate the balancing act of complying with applicable, and sometimes conflicting, sanctions and countermeasures.

Contacts



Ronin Zong
Partner

rlz@wrco.com.cn



Therese Trulsen
Specialist Counsel

ttr@wr.no






Bård B. Bjerken
Senior Lawyer

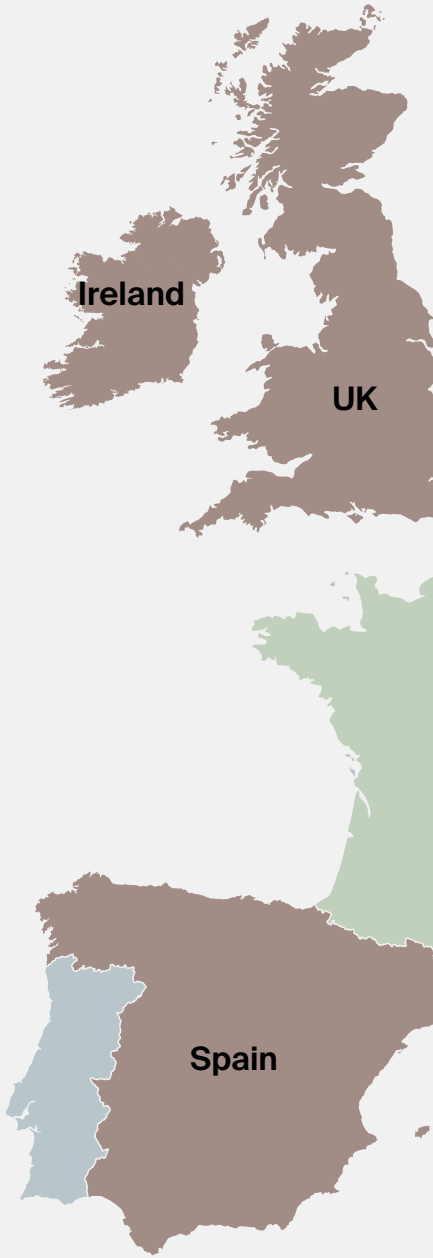
bbb@wrco.com.cn

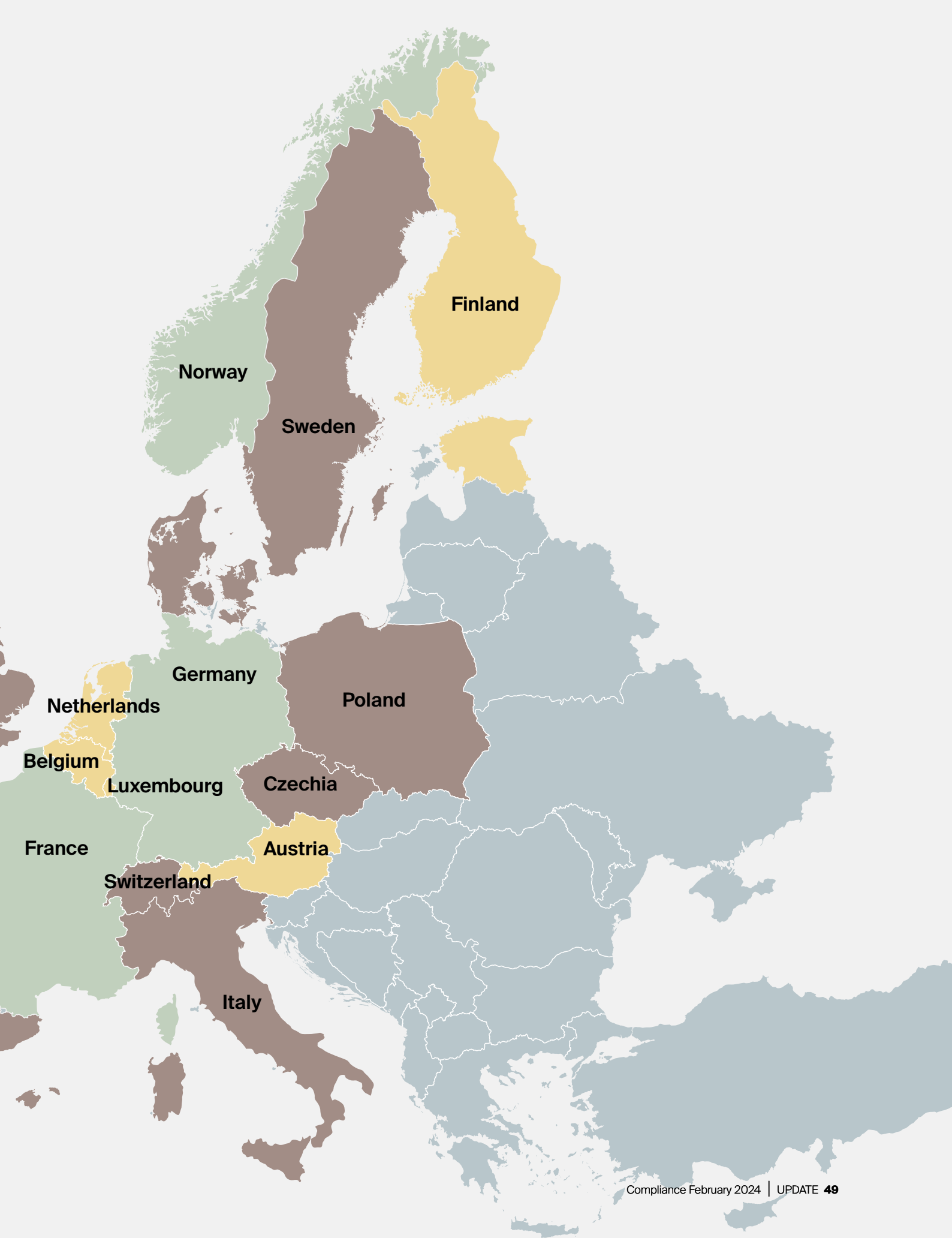


Status: mandatory human rights and environmental due diligence

Regulatory requirements to conduct human rights and environmental due diligence have been or are on the verge of being implemented in several EU countries. Although there are differences, taking a pan-European approach to due diligence requirements can often provide significant efficiency gains. This map depicts the status of legislative processes in this area in various European countries. In addition, on EU level, there is a proposal for the EU Corporate Sustainability Due Diligence Directive.

-  Final act implemented
-  No law, but on the legislative or political agenda
-  Draft law issued





”A true one-stop shop for complex cross-border compliance matters and crisis management.”

Legal 500



Wikborg Rein’s compliance practice – contact list

OSLO

Partners

Elisabeth Roscher
elr@wr.no / +47 90 94 76 15

Tine E. Vigmostad
tv@wr.no / +47 95 28 12 64

Kristin N. Brattli
knh@wr.no / +47 95 84 87 38

Elise Johansen
elj@wr.no / +47 41 62 80 99

Gry Hvidsten
ghv@wr.no / +47 90 94 76 15

Arild Frick
af@wr.no / +47 90 68 18 44

Oddbjørn Slinning
osl@wr.no / +47 481 21 650

Ole Andenaes
oea@wr.no / +47 93 26 70 67

Geir Sviggum
gsv@wr.no / +47 91 11 18 41

Jan L. Backer
jlb@wr.no / +47 91 37 58 15

Mads Magnussen
mma@wr.no / +47 93 21 59 83

Preben Milde Thorbjørnsen
pmt@wr.no / +47 41 64 93 40

Aadne M. Haga
aha@wr.no / +47 91 62 88 20

Specialist Counsels
Therese Trulsen
ttr@wr.no / +47 92 08 18 60

Jens Fredrik Bøen
jfb@wr.no / +47 95 55 29 96

Tonje H. Geiran
tog@wr.no / +47 95 20 65 05

Stuart Stock
sts@wr.no / +47 48 28 78 12

Senior Lawyers
Hanne R. Gundersrud
hgu@wr.no / +47 46 82 94 59

Johan A. Heber
jah@wr.no / +47 93 69 92 91

Kristina Nettet Kjerstad
knk@wr.no / +47 99 42 45 48

Elin G. Opheim
ego@wr.no / +47 48 13 90 96

Julia Skisaker
jsk@wr.no / +47 90 58 42 76

Kristina N. Kjerstad
knk@wr.no / +47 99 42 45 48

Senior Associates
Karoline Angell
ang@wr.no / +47 91 34 91 93

Ingrid Weltzien
iwe@wr.no / +47 98 81 50 96

Øyvind Rishoff
oyr@wr.no / +47 95 70 42 92

Patrick Oware
pkow@wr.no / +47 47 85 51 43

Associates
Marie Hatten
mht@wr.no / +47 99 12 43 91

Åshild Eliassen
ase@wr.no / 47 23 84 02

Mads K. Haugse
mau@wr.no / +47 48 00 88 87

Noor Kahn
nkh@wr.no / +47 93 61 54 04

Maren Folkestad
mfo@wr.no / +47 99 10 01 01

Emily E. Andersen
ead@wr.no / +47 98 06 61 79

Camilla P. Fjeldstad
cpf@wr.no / +47 41 62 67 20

Shahin Fashkhami
shf@wr.no / +47 92 83 72 12

Project Assistant
Anja Kirkeby
aki@wr.no / 22 82 77 42

BERGEN

Senior Associates
Bendik Torset
bto@wr.no / +47 99 34 83 66

Heidi Ann Vestvik-Bruknapp
hbk@wr.no / +47 41 57 54 17

Associate
Guro Bjørnes Skeie
gbs@wr.no / +47 455 06 485

LONDON

Partners
Renaud Barbier-Emery
rbe@wrco.co.uk / +44 78 8959 8672

Chris Grieveson
cjg@wrco.co.uk / +44 79 6644 8274

Shawn Kirby
skk@wrco.co.uk / +44 78 4169 7476

Baptiste Weijburg
baw@wrco.co.uk / +44 78 4148 1102

Counsel
Beatrice Russ
bru@wrco.co.uk / +44 7756 285 154

Consultant
Eleanor Midwinter
elm@wr.no / +44 7841 422 690

Specialist Counsels
Matt Berry
mat@wrco.co.uk / +44 77 0971 6541

Olga Ivanov
olv@wrco.co.uk / +44 7521 757 177

Senior Lawyers
Fiona Rafia
fra@wrco.co.uk / +44 7841 470 380

Amanda Urwin
aur@wrco.co.uk / +44 7756 288 8751

Sophie Henniker-Major
soh@wrco.co.uk / +44 7756 289 541

Senior Associate
Sebastian Bergeton Sandtorv
sbs@wrco.co.uk / +44 20 7367 0325

Associate
Jack Wray
jwr@wrco.co.uk / +44 7596 566 221

Trainee Solicitor
Iliana Mastoraki
iam@wrco.co.uk / +44 6598 611 257

Lina Malone
lm@wrco.co.uk / +44 7511 179 511

SHANGHAI

Specialist Counsel
Xiaomin Qu
xqu@wrco.com.cn / +86 135 6475 3289

Senior Lawyer
Bård B. Bjerken
bbb@wrco.com.cn / +86 185 2132 1616

Senior Associate
Sherry Qiu
shq@wrco.com.cn / +86 135 0171 2717

SINGAPORE

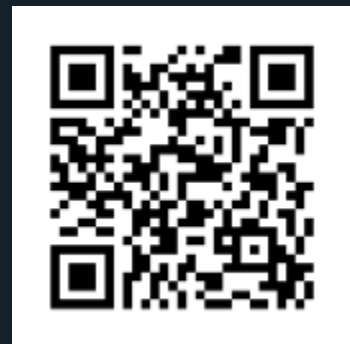
Partner
Wole Olufunwa
wol@wr.com.sg / +65 8030 0380

Ina Lutchmiah
ivl@wr.com.sg / +65 9662 3756

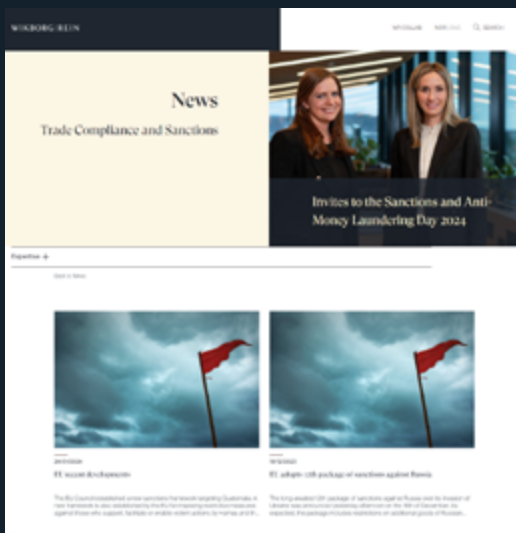
Alert services free of charge

WR Sanctions Alerts provide updates on material developments in sanctions programmes implemented by the EU, UK, US and Norway.

WR ESG Alerts is a monthly newsletter that covers key developments on topics of relevance under the ESG umbrella.



Scan the QR code to sign up for our alerts



WIKBORG | REIN

wr.no

OSLO | BERGEN | STAVANGER | LONDON | SHANGHAI | SINGAPORE