Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
CSLR – EU update – April 2020

Imogen Palmer, Kit Burden*

DLA Piper, United kingdom

ARTICLE INFO

Keywords:
EU
Technology
Outsourcing
Coronavirus

ABSTRACT

Relevant DLA Piper articles published since the previous submission in February.

1. EU data protection: COVID-19

By Andrew Dyson, Partner and Patrick Van Eecke, Partner, DLA Piper Leeds and Brussels

The world is facing unprecedented challenges in its fight to contain the Coronavirus (COVID-19). Various countries are in lockdown and emergency measures being implemented to contain the pandemic, with European countries currently at the epicentre of the outbreak.

Organisations are looking to adopt measures that support business continuity, whilst appropriately protecting the health and safety of workers and customers, and complying with wider public health initiatives. The pace of response is fast moving, as the impact of the pandemic spreads quickly.

1.2. Application of the GDPR

As organisations implement emergency measures, it is important to be aware of the privacy implications of any steps being taken. In the EU, any measures which involve processing of personal data are likely to give rise to data protection compliance issues that will need to be managed consistent with the General Data Protection Regulation (GDPR).

The following are examples of some common measures being adopted by organisations which will give rise to processing of personal data and (in many cases) information about an individual’s state of health which is subject to additional regulation as ‘special category personal data’ under the GDPR:

- dealing with members of the workforce who are suffering from COVID-19, or who may be at risk, or who may have vulnerable family members;
- tracing people who have been in contact with someone who has tested positive for COVID-19, or may otherwise be at high risk;
- asking staff to complete questionnaires asking about potential exposure to the virus, or underlying health conditions or vulnerabilities which may present enhanced risks;
- carrying out temperature checks on entry to sites; and
- sharing information with public health authorities.

It is important to understand that the GDPR applies to these and similar response activities and there is no general waiver for compliance because we are dealing with a public health emergency. Compliance officers should bear this in mind and ensure that where measures are being adopted the

* Corresponding author. Kit Burden, DLA Piper, United kingdom.
E-mail address: kit.burden@dlapiper.com (K. Burden).

https://doi.org/10.1016/j.clsr.2020.105434
0267-3649
usual principles are followed to ensure processing is fair, lawful and transparent, necessary and proportionate with minimal levels of data captured for the required purposes and due confidentiality and retention controls applied.

### 1.3. Lawful conditions for processing data

In many cases, a key question will be what lawful basis applies under Article 6 of the GDPR and (in the case of health data being processed) Article 9. The most relevant Article 6 grounds are likely to be:

- “vital interests”: the processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- “legitimate interests”: the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data; or

Where processing involves health data, relevant Article 9 grounds include the following (noting that explicit consent is generally not going to be valid in respect of employees):

- “preventative and occupational medicine”: the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law (Art 9(2)(h));
- “public health”: the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health... on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Art 9(2)(i)); and
- "employment law": the processing is necessary for the purposes of carrying out rights of the controller or data subject in the field of employment... insofar as it is authorised by Union or Member State law. (Art 9(2)(b)).

As the text above notes, this aspect of the GDPR is devolved to Member States with limited EU level harmonisation. This means local privacy and employment laws will need to be checked to understand the extent to which specific measures may be validly adopted on a per country basis when processing health data.

### 1.4. Response from data protection supervisory authorities

Regulators are aware of the challenges in this area and the risk that GDPR inadvertently prevents organisations taking necessary and appropriate measure to protect individuals from the pandemic. Over the space of a week almost all EU regulators issued guidance on this issue, but the guidance is not consistent. The general theme is to explain that GDPR standards still apply throughout the pandemic and note the key provisions that need to be addressed, encouraging organisations to be thoughtful about collecting excessive data and ensure health data in particular is not collected unless a special condition can be met. Most recognise the enhanced pressures that the pandemic brings and in some cases indicate that any shortfalls in compliance during the current period will be considered appropriately when considering enforcement. This may give some assurance to risk based decisions that are inevitably going to be made.

Critically, some regulators have set out quite limited interpretations of the GDPR for key activities which we know are taking place routinely – for example stating that measures such as thermal checking and medical questionnaires should be reserved for public health authorities only, or must be conducted under the direct supervision of a health professional. In some cases, this guidance is being superseded by emergency legislation, which includes specific legal gateways relaxing these controls through further derogations to the Article 9 conditions.

### 1.5. Key takeaways

Businesses should consider taking the following steps when in response to the privacy risk associated any additional COVID-19 processing activities:

1. Ensure that measures implemented are consistent with current (and rapidly evolving) public health advice. This advice will inform what is necessary/proportionate under GDPR.
2. Limit the nature and volume of additional personal data processing activity to that absolutely necessary to carry out the relevant response measure. Wherever possible avoid processing specific health related information which can be linked back to an individual.
3. Ensure measures are strictly time limited to dealing with the current pandemic and curtailed once no longer necessary.
4. Ideally have all additional measures supervised and signed off by a health care professional/occupational health professional, in particular if health data are being processed.
5. Display a notice to explain what data is being collected, by whom and for what purposes and (as appropriate) update privacy policies.
6. Maintain a record of the lawful basis for processing.
7. Comply with the other relevant GDPR principles on retention, security etc.
8. Record the decision making in a data protection impact assessment.
9. When dealing with workforce data and related decisions, also consider compliance with employment laws and understand the impact on workforce rights, pay etc.

This article was first published on, and was accurate as of, 1 April 2020. Please refer to our website (www.dlapiper.com) for further insights in light of daily global developments.
2. Is coronavirus a force majeure event (in England and Wales)?

By Stephen Wright, Partner, David Booth, Senior Associate, Adam Kelly, Associate, Tahir Cheema, Associate, and Clare Bayliss, Associate, DLA Piper Manchester and Liverpool

These straightforward FAQ explain what force majeure provisions are, how they work, and whether coronavirus is a force majeure event. This guidance covers the force majeure position in England, Wales and Scotland (which all work the same way), but will be relevant to a wider audience, because many international commercial contracts have a provision stating they are governed by the law of England and Wales. Before we get to COVID-19, let us start with the basics.

2.1. What is a force majeure provision?

Force majeure provisions are contractual clauses that offer relief from performing some or all of the obligations in a contract. They usually apply when specified events occur: essentially, events beyond the control of the affected party that prevent them from performing some or all of the contract.

Force majeure is a contractual remedy under English law. So if a contract is silent on force majeure, English law will not imply it into the contract. Similarly, undefined references to force majeure in an English law contract, without any contractual definition or interpretation, will not have an implied definition at law.

This is different to some other (often civil-law) legal systems where force majeure is a legally defined concept and where courts may declare that a particular event, such as coronavirus, is a force majeure event.

Force majeure is typically not a feature in property leases.

2.2. When can I rely on force majeure?

If the contract does not have a force majeure provision, you cannot rely on force majeure.

If the contract does have a force majeure provision, the interpretation of it is fact-specific and contract-specific, so it is important to get legal advice early.

Generally speaking, you can rely on a force majeure event where it prevents or delays (to the standard required by the provision) your ability to perform your obligations under the contract.

It is highly unlikely you had been able to rely on a force majeure provision simply because performance is more expensive, difficult or commercially undesirable.

Where part but not all of a contract is affected by a force majeure event, you and the other party should (unless the relevant provisions provide otherwise) continue to perform the unaffected part of the contract (including making payment of relevant charges). This is because, from a legal perspective, that unaffected part of the contract will continue to operate in full force and effect.

2.3. What else must I consider when interpreting my force majeure provision?

All force majeure provisions must be considered and interpreted by reference to the other related provisions in the contract. An example of a related provision is the interpretation provision. “Force Majeure” definitions in contracts often contain lists and examples of applicable events. These must be reviewed to establish:

- whether any words like “including” or “for example” mean that the list of force majeure events should be read as an exhaustive or non-exhaustive list; and
- whether the examples in the definition are intended to limit the list or not – for example, depending on the interpretation provision, an “act of god” will probably include COVID-19, but the same phrase followed by a list of examples that all relate to meteorological events may not.

2.4. Is coronavirus a force majeure event?

As above, the language of a force majeure provision typically identifies the events or circumstances in which the provision will apply. These are usually set out in a list of “force majeure events.” The events in this list can be either specific or more general, but typically they are all things beyond the reasonable control of the affected party.

Subject to the guidance above on interpretation:

- lists that include “epidemic” and/or “pandemic” will likely cover COVID-19;
- other events or circumstances such as “acts of government,” “acts of god,” “acts of nature” and “civil emergency” (among others) may cover coronavirus; and
- events stated to be “beyond a party’s reasonable control” are also likely to cover COVID-19.

However, none of the points in the three bullets above have been tested yet in the courts.

Even if COVID-19 is within the scope of your force majeure provision, before claiming force majeure you must consider carefully the impact of coronavirus on your ability to perform your contractual obligations and whether that impact meets the standard required by the provision. See above and below in this note for guidance on these points.

2.5. Is fault relevant to force majeure?

Unless the force majeure provisions in the specific contract provides otherwise, if there is fault attributable to a party, this suggests that the circumstances are not beyond the reasonable control of that party and, therefore, that force majeure is not relevant.

2.6. Does mitigation apply to force majeure?

Force majeure provisions often require the party seeking the relief to demonstrate they have mitigated, to the extent possible, any impact.
Also be aware that in many (but not all) cases, English law implies a provision into contracts obliging a party suffering loss to mitigate that loss.

2.7. **How does business continuity and disaster recovery relate to force majeure?**

Often, a well-drafted force majeure provision will stop a party relying on it if that party did not operate the business continuity/disaster recovery provisions of the relevant contract.

Where a force majeure provision is silent on this matter, the extent to which a party did not operate the business continuity/disaster recovery provisions of the relevant contract are likely to be considered as part of the question of mitigation (see the preceding section).

2.8. **So, in summary, what is required to rely on a force majeure provision?**

Each force majeure provision is worded differently, but typically you'll need to show that:

- the force majeure event is within the scope of the provision;
- non-performance or delayed performance was caused by the force majeure event and/or events outside your control; and
- you have attempted to mitigate the effects of the force majeure event.

2.9. **Can force majeure help exclude or delay making payment?**

Unless the banking system collapses or some other force majeure event happens that actually prevents payment being made, it is unlikely that as a customer you had been able to successfully rely on force majeure to excuse or delay making payments under a contract (and often, the contract will specify this explicitly).

That does not mean you had need to pay for goods or services you do not receive due to a supplier being affected by a force majeure event – that would be highly unlikely under English law. But you had be wise to make suspension of relevant payment obligations clear in any force majeure provisions, including an entitlement to refunds or credits if payments are to be made in advance.

Typically, force majeure is a remedy that benefits suppliers, as they tend to be responsible for most of the obligations related to performance, rather than customers, whose principal obligation is often confined largely to payment.

If the force majeure event affects only parts of the contract then, as noted above, a customer will be required to pay for the unaffected goods or services it receives.

2.10. **What happens to the contract when I invoke the force majeure provision?**

This depends on the language of the provision. Typically, the affected party is excused from performing the affected obligations under the contract. However, provisions typically allow the unaffected party to terminate only after a specified period – see the next section below.

Exercise caution and take advice before invoking a force majeure provision: doing so where there is no force majeure event (as defined in the contract) may entitle the other party to claim that the contract has been breached, terminate it and claim for damages.

Sometimes, force majeure provisions are drafted to give termination rights to both the unaffected and affected parties.

2.11. **When can I terminate under a force majeure provision?**

Termination rights are usually triggered (usually for one party, but sometimes for both) only where the force majeure event persists for a specified period of time, and only after this period may the party terminate the contract. A party seeking to invoke the force majeure provision to terminate the contract should also strictly follow the provision's notice requirements; failing to do so could render the termination ineffective, if the other party disputes it.

2.12. **Is force majeure my only possible remedy?**

No. To assess the options available to you, a full review of the relevant facts and the contractual provisions should be carried out. Often, other clauses are as relevant – or even more relevant – than force majeure.

Here is a non-exhaustive list of other contractual provisions/regimes that could be relevant in circumstances when force majeure is being considered:

- business continuity and disaster recovery (see above);
- customer responsibilities and dependencies, relief events and excusing causes;
- changes in law;
- material adverse change;
- most-favoured customer and minimum purchase/sale commitments;
- liquidated damages and time of the essence;
- set-off;
- step in;
- financial distress; and/or
- termination.

Affected parties should also consider their non-contractual remedies, for example under the doctrine of frustration – see the next section.

2.13. **What is the doctrine of frustration?**

If a contract does not have a force majeure provision that deals with the event in question, an affected party should consider whether they have a potential remedy under the common-law doctrine of frustration.

For frustration to apply, an unforeseen event must happen that is neither party's fault but that makes the performance of the contract impossible or radically changes the nature of the contract from what was intended when the parties entered.
into it. If proved, the remedies are similar to force majeure relief – but frustration is typically very difficult to prove.

If a contract has force majeure provisions that deal with the relevant event, frustration is unlikely to be applicable.

3. Coronavirus COVID-19 and frustration: is your contract at risk? (England and Wales)

By Jamie Curle, Partner, and Charles Allin, Senior Associate, DLA Piper London

The ongoing global coronavirus COVID-19 outbreak is creating uncertainty and difficulty for enterprises worldwide, particularly those whose business depends on large gatherings of people. The below gives such businesses guidance on protecting their legal rights and mitigating the worst economic effects of the virus.

Businesses are keen to understand how their contractual position might be affected by the coronavirus COVID-19 outbreak and what remedies might be available if it becomes difficult or impossible for their counterparties to perform their obligations. One potential remedy may be contractual force majeure provisions. Another is the doctrine of frustration, which may be relevant if the contract contains no force majeure clause covering coronavirus COVID-19 issues.

Frustration is difficult to prove, but where an extreme event like the current coronavirus COVID-19 outbreak occurs, you are more likely to see counterparties seeking to rely on it to extricate themselves from difficult contractual arrangements. You should, therefore, consider whether the coronavirus outbreak might place your contracts at risk or provide you with an opportunity to exit on frustration grounds, and what your response to, or case for, frustration might be.

3.1. What is frustration?

Under English law the doctrine of frustration allows a contract to be discharged when an unforeseen event occurs that renders the performance of the contract impossible. The purpose of frustration is to avoid injustice where there has been a significant change in circumstance and neither party is at fault. Where a frustrating event occurs, the contract is automatically terminated by operation of law without requiring any action of the parties.

3.2. When will a contract be frustrated?

The threshold for frustration is very high, and the test is strict. A contract may be frustrated where:

- the frustrating event occurs after the contract has been formed;
- the event is beyond what was contemplated by the parties on entering the contract and is so fundamental that it strikes the root of the contract;
- neither party is at fault; and
- the event renders performance of the contract impossible, illegal or radically different from what was contemplated by the parties at the time.

In considering the last point, all relevant factors must be taken account of, including the contractual terms and the factual background – particularly the question whether the parties considered what would happen (and whether the contract would be performed) if the frustrating event occurred. In the context of leases, whilst frustration could technically apply to a lease, this is likely to be very difficult to prove in practice.

3.3. Will the coronavirus outbreak frustrate your contract?

You’ll need to consider the terms and background of each of your contracts individually. The key question is whether the coronavirus COVID-19 outbreak makes performance of a contract impossible, or only more difficult. The latter will not result in the contract being frustrated. For example, if the coronavirus COVID-19 outbreak merely delays performance of an obligation, or increases the cost of doing it, it is highly unlikely frustration will apply. Similarly, if coronavirus COVID-19 results in a tenant being temporarily unable to occupy its premises in England, it is unlikely that it will be able to argue successfully that its lease has been frustrated.

3.4. Frustration or force majeure?

Generally, where a contract contains a force majeure clause that engages specifically with the issues raised by the coronavirus COVID-19 outbreak that are said to give rise to frustration, frustration will not apply, because the parties have already considered that issue and provided for it in the contract. However, if the force majeure clause is not full, complete or specific enough (e.g. there is room for debate on whether it covers the event in question), it may still be possible to invoke frustration.

3.5. Should you argue frustration?

Both force majeure and frustration offer contractual parties relief from their obligations. But there is a crucial difference: a force majeure event may not result in the contract being terminated (it simply relieves a party from complying with the obligation subject to force majeure), whereas frustration results in automatic termination.

Depending on your rights and obligations under the contract, it may not be commercially astute or legally appropriate to invoke frustration – for example, where the contract contains long-term rights and obligations that will not be rendered impossible by the temporary effects of the coronavirus COVID-19 outbreak.

Further, the consequences of wrongfully asserting frustration may be severe: a mistaken allegation may amount to an anticipatory or repudiatory breach of the contract, which may result in the counterparty itself terminating the contract and claiming damages. You should, therefore, give careful consideration and take legal advice before asserting frustration.
4. **AI outlook: Europe initiates AI regulation introducing the principle of trustworthy AI**

By Patrick Van Eecke, Partner, Valerijus Ostrovskis, Senior Associate, Thomas Gils, Associate, and Laura Semmler, EU Policy Advisor, DLA Piper Brussels

On February 19, 2020, the European Commission presented its White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, a much-anticipated policy document setting out concrete measures and proposed regulation with the objective of promoting the development, uptake and use of AI applications, while also addressing the resulting fundamental rights challenges.

The document has raised concerns among companies about whether new rules on AI will negatively impact businesses developing or deploying AI solutions across the EU. Feedback on the white paper can be provided until May 19, 2020.

4.1. **Key elements of the white paper on AI**

The white paper proposes a dual approach. It aims to establish an “ecosystem of excellence” on the one hand, and an “ecosystem of trust” on the other hand.

4.1.1. **Ecosystem of excellence**

To promote the development and uptake of AI applications by European citizens, businesses and public institutions, the Commission proposes to:

- encourage synergies among centres for research and innovation to reduce fragmentation (including the creation of testing and experimentation sites for AI applications);
- further enhance cooperation between EU Member States;
- support upskilling initiatives for the workforce;
- promote adoption of AI solutions across sectors and organizations of various sizes (particularly SMEs); and
- expand investment in AI development and deployment.

The European Data Strategy, published alongside the white paper, aims to create a European single market for data, to facilitate access to data and computing infrastructures – an essential requirement for the development and use of AI applications.

4.1.2. **Ecosystem of trust**

To address the challenges development and deployment of AI applications may pose in relation to fundamental rights, safety and other obligations, the white paper suggests concrete regulatory options. Importantly, the document states that the relevant EU legal framework should be principles-based and target so-called “high-risk AI systems”.

The document underlines that existing EU laws and regulations already apply to AI solutions, including rules on data protection (GDPR), consumer protection, safety and liability. The Commission asserts, however, that the AI-related aspects of these existing rules may be difficult to enforce due to the typical characteristics of AI systems, such as opacity, unpredictability, complexity, and autonomous behaviour. Against this background, the Commission proposes to evaluate individually the need for legislative amendments or the introduction of new legislation, on the basis of the identification of specific risks.

4.2. **Envisaged scope of application**

With a view to such potential future regulation of AI, the white paper takes a risk-based approach (similar to that of GDPR), particularly by singling out “high-risk applications”, which could become subject to the most stringent requirements. The Commission says that an AI application should be distinguished as “high-risk” if two cumulative criteria apply:

- **The sector involves significant risk:** this will be the case if, given the characteristics of the activities typically undertaken in that sector, significant risks can be expected to occur. The white paper states that these sectors should specifically and exhaustively be listed in the potential future legislation, mentioning the examples of healthcare, transport, energy and parts of the public sector.
- **The intended use involves significant risk:** this entails that the AI application in the sector in question should be used in such a manner that significant risks are likely to arise. By including this second criterion, the Commission aims to acknowledge that not every use of AI in the selected sectors necessarily involves significant risks that would in turn justify legislative intervention.

Importantly for companies, the white paper proposes to introduce certain exceptions, irrespective of the sectors concerned, where the use of AI applications would be considered as “high-risk as such” (e.g. facial recognition technology or for recruitment purposes).

4.3. **Envisaged obligations for high-risk AI applications**

The Commission proposes that the future regulatory framework for high-risk AI applications could impose mandatory legal requirements on the below key aspects (which echo the requirements set out by the AI HLEG in its Ethics Guidelines):

- **Training data:** the Commission considers requirements regarding the quality of training data (representative and comprehensive data-sets) and compliance with privacy and data protection rules.
- **Data and record-keeping:** the paper considers the introduction of requirements to keep records of the selection process and the characteristics of training and testing data, and the methodologies used for programming and training. These records should enable regulatory review and enforcement by allowing AI decisions to be traced back and verified.
• **Information to be provided:** the document recommends requirements related to transparency (e.g. information provision on capabilities and limitations of AI systems), and a notice requirement when citizens would interact with an AI system rather than a human being.

• **Robustness and accuracy:** the Commission considers requirements on robustness and (the level of) accuracy, reproducibility of outcomes, ability to react to errors and inconsistencies, and resilience against attacks and manipulation of data or algorithms.

• **Human oversight:** the white paper considers the imposition of some degree of human oversight and suggests targeted requirements, depending on the specific circumstances, ranging from requiring human review before a decision is implemented, to the possibility of human intervention in real-time or afterwards.

• **Specific requirements for remote biometric identification (i.e. facial recognition):** a ban of three to five years on facial recognition technology was considered in an earlier, leaked draft version of the white paper, featuring prominently in the public debate over the past weeks. In the official version of the document, however, the Commission took a step back, no longer proposing a concrete ban, but referring to current EU data protection rules and the Charter of Fundamental Rights, which already allow the use of remote biometric identification only in cases where this action is justified and proportionate, and is subject to adequate safeguards. As a next step, the Commission wishes to engage in a public discussion on potential exceptions – if any – that might justify the use of AI for remote biometric identification.

As such requirements would be imposed on “high-risk” AI applications, the Commission suggests a prior conformity assessment, possibly including procedures for testing and inspection of certification of algorithms and data sets. For AI applications that would not be identified as “high-risk,” the Commission is considering a voluntary labelling system that would certify compliance with (parts of) the requirements and allow companies to market their AI products as “trustworthy”.

### 4.4. Expected business implications

The additional policy and regulatory measures considered in the white paper will increase the cost of compliance and the administrative burden on companies operating in a variety of sectors when they develop or deploy AI systems.

The suggested requirement for firms to possibly submit their AI products and services to a conformity assessment before being allowed entry to the EU market would significantly increase the costs and time required for firms to deploy new AI applications, and might pose IP-related difficulties.

By proposing the introduction of the two cumulative requirements of (i) belonging to a certain high-risk sector, and (ii) being intended for a certain high-risk use, the Commission seeks to avoid designating full sectors as “high-risk” while taking into account that the level of risk associated with the use of AI applications in a specific sector may range from low- to high-risk applications. However, this approach may also lead to uncertainty, as some AI-applications may be considered high-risk in one sector but not in another, and in order to determine this, further detailed regulatory guidance will likely be required.

Further, a major uncertainty for companies developing or deploying AI applications lies in the Commission’s consideration of “certain exceptions”, where the use of an AI application would be considered to be “high-risk as such”.

### 4.5. Next steps

The European Commission’s public consultation on the white paper on AI runs until May 19, 2020.

The European Parliament is also working on a number of AI-related policy and legislative dossiers with major implications for organizations. These files cover aspects of AI in relation to:

- civil liability (request for a legislative proposal);
- intellectual property (report);
- education, culture and audiovisual (report);
- ethics (request for a legislative proposal);
- criminal law (report); and
- international law/civil and military use (report).

The reports may feed into a motion for a resolution, which would allow the European Parliament to direct the Commission’s and Member States’ attention to the matter. The requests for a legislative proposal – if agreed by the Commission – will trigger the Commission to initiate legislation.

Organizations should closely monitor these developments, and engage with the relevant decision-makers to ensure that their interests are represented.

### 4.6. What other commission initiatives will affect the digital sector over the coming months?

The AI white paper was presented as one of the two initial pillars of a far-reaching EU Digital Strategy that sets out the Commission’s key objectives in the field of digital for 2020–2024. The second pillar is a European Strategy for Data, which aims to enhance the use of data by creating an EU single market for data. In parallel, the Commission published its report on the safety and liability implications of AI, the Internet of Things and robotics.

Moreover, the European Commission’s 2020 Work Programme contains several additional relevant initiatives that will considerably affect companies operating across the EU. The most notable initiatives for launch in Q1 of 2020 include the publication of a new industrial strategy and a dedicated SME strategy.

### 4.7. Previous EU activities related to AI

The political guidelines for the new European Commission (2019–2024) under Commission President Ursula von der Leyen initially announced the introduction of binding legislation on a “coordinated European approach on the human and ethical implications” of AI in a broad range of sectors. The AI white paper now indicates that the process of regulating
AI has been slowed down. Instead of binding legislation, the Commission has put forward a non-binding policy document, which, however, does contain concrete proposals for AI regulation.

The 2020 Commission Work Programme, a document published annually and presenting the Commission’s key policy and legislative initiatives for the upcoming year, reiterates that binding legislation on AI will be proposed in Q4 of 2020, in particular regarding safety, liability, fundamental rights and data aspects.

These developments follow the AI-related activities of the previous European Commission, undertaken in cooperation with the EU Member States. Since April 2018, all Member States have committed to a Declaration of cooperation on AI, and a European AI Strategy has been concluded.

EU Member States have agreed a Coordinated Action Plan on AI, which will be updated in 2020. Apart from the Ethics Guidelines, the AI HLEG has also put forward policy and investment recommendations for Trustworthy AI. Another expert group compiled a report on liability for AI and other emerging technologies, containing suggestions for updates to EU and national liability regimes.

5. AI-Enabled innovation, part 1: regulatory intervention and AI in financial services

By Mark Rasdale, Partner and Cezary Bicki, Associate, DLA Piper Dublin

5.1. The big data challenge

There has recently been an indication that the Data Protection Commission (DPC) in Ireland will increase its focus on ensuring privacy by design and default during 2020. From the regulator’s perspective innovation is encouraged, provided it is done in an accountable, ethical and fair way. Already, with the codification of Privacy Impact Assessments and accountability under the GDPR, businesses are realising that key decision makers in the organisation ought to be fully briefed on how risks are mitigated in relation to Big Data and artificial intelligence (AI) – enabled technology projects.

The promise of new technology, such as AI – based automation and enhancement has turned many businesses into data hoarders. That approach might not work for long as the EU recently urged European businesses to capitalise on their vast data resources. The use of AI solutions is one way to do so. The holy grail for many financial services (FS) firms in particular, is the single customer view; mine the data for knowledge and automate delivery, in order to enhance the relationship with the customer. This can be achieved, but not without large databases of quality data and very sophisticated technology solutions. Investment in both continues to grow.

5.2. AI leaders in financial services

49% of AI frontrunners in FS have a comprehensive and detailed AI strategy
45% of AI frontrunners are investing over 15% in AI initiatives
60% of AI frontrunners define AI success by improvements to their revenue and 47% by improving customer experience

5.3. Legislating for AI

Much of the focus in terms of regulatory and compliance risk in relation to AI – enabled innovation is around privacy. But that lens is too narrow. Indeed, current EU legislation on data protection, competition and consumer protection does not define ‘big data’ clearly or at all, which arguably creates a regulatory blind spot that will need to be addressed.

The EU is advocating for the need to prepare for the socioeconomic changes brought by AI and to ensure an appropriate ethical and legal framework for it. Last year, the EU Commission published the Ethics Guidelines for Trustworthy Artificial Intelligence and the Report on liability for Artificial Intelligence and other emerging technologies. Expect more during 2020 from the Expert Group on Liability and New Technologies, particularly in relation to whether existing legal frameworks, such as the product liability regime, is fit for purposes when it comes to AI enabled products.

The state of country level regulatory activity in relation to AI currently remains varied across Europe. However, the regulators and legislators in most countries recognise the importance of AI and have started formulating their policies.

In the US, the White House issued guidelines for federal agencies on how to approach AI regulation, and it emphasises the need for proportionate approach where less regulation may be preferred.

---

1 Financial Times, Europe urged to use industrial data trove to steal march on rivals, https://www.ft.com/content/8187a268-3494-11ea-a6d3-9a26f8c3cba4, accessed 15 Jan 2020.

2 Deloitte Development LLC, Deloitte Insights, AI Leaders in financial services, 2019, https://www2.deloitte.com/content/dam/insights/us/articles/4687_traits-of-ai-frontrunners/DI_AI-leaders-in-financial-services.pdf, accessed 10 Jan 2020.
“Fostering innovation and growth [of AI] through forbearance from new regulations may be appropriate”

The recently proposed Algorithmic Accountability Act 2019, while still in draft, is an example of a concrete legislative attempt in the US to address concerns in relation to ethical and accountable use of AI. It would require bias and security impact assessments (thereby going beyond privacy concerns) to be conducted by a wide range of players prior to implementing new AI based product and service.

Much of the regulatory activity internationally is being informed by OECD’s values of trustworthy AI, which include: AI driving inclusive and sustainable growth, diversity and fairness, transparency, security, and accountability.3

5.4. Regulatory guidance in the financial services sector

In relation to financial services, we think the distinction between privacy and more 'general' regulation will be increasingly blurred due to more co-operation and convergence between the two regulatory competencies in relation to AI – enabled innovation.

As the old adage goes, you will get out of [AI] what you put in to it. Bad, unstructured data makes for unsatisfactory results and sometimes additional risk.

The Central Bank of Ireland (CBI) has publicly stated that there is a significant challenge with data sourcing and management amongst firms it regulates:

“Firms need to have a single source of their key data if they are to rely on it for critical intelligence and decision-making. Those that manage this transition best are likely to be the firms that survive and thrive.”4

In other words, banks and other financial services firms need to substantially invest more in their technology and data capabilities. Effective management of technology risk requires IT systems that are integrated and up to date. Data cannot be captured, interrogated and exploited in business and operational silos. The governance, legal and risk management structures and skill sets in financial services firms should not be playing a catch-up with the technological innovation.

The CBI is not alone in expressing such views. Just like the potential of AI technology, the regulatory challenges and perspectives around AI are also borderless.

The Monetary Authority of Singapore (MAS) has confirmed that when used responsibly and effectively, AI has significant potential to improve business processes, mitigate risks and facilitate stronger decision-making. It worked closely with the Personal Data Protection Commission (PDPC) to develop a set of principles for firms to use in their internal governance structures to govern use of technologies that assist or replace human decision-making.5 The principles are built around four key concepts and below we give a brief outline of each, an example of how failure to adhere to such principles might manifest itself when using AI in financial services and a possible risk mitigant:

### Table

| Principle | Rationale for Principle | AI Use Case | Risk Mitigant |
|-----------|------------------------|-------------|--------------|
| Ethics    | That AI – enabled decisions are aligned to the companies’ own code of conduct and are held to at least the same ethical standard as human decisions. | Advancements in conversational AI make it difficult to distinguish interactions with digital assistant tools from real human to human interaction. | Implement controls during the data preparation and feature engineering phases to detect and prevent bias and discrimination. Use data skewness analysis to the training dataset to verify that the different classes of the target population are equally represented (e.g. oversample under-represented classes). Use crafted data sets to test models against discriminatory behaviour and regularly monitored the AI system in production to ensure that it does not display discriminatory behaviour. |
| Fairness  | That decisions are regularly reviewed and validated for accuracy and relevance, and to minimize unintentional bias. | A credit score decision is generated to predict suitability for new credit (and related interest rates) based on prior repayment history and other unstructured external data sources. The output is affected by the bias in the algorithm and data and disproportionately ranks women lower than men and favours certain customer classes over others. | Include a notification at the start of interaction to indicate the customer is engaging with an automated assistant, speaking on behalf of the human and giving an option to divert to human interaction. |

(continued on next page)

---

3 OECD Principles on AI, [https://www.oecd.org/go/going-digital/ai/principles/](https://www.oecd.org/go/going-digital/ai/principles/), accessed 15 Jan 2020.

4 The need for resilience in the face of disruption: Regulatory expectations in the digital world – speech Deputy Governor Ed Sibbey, 09 October 2018, [https://www.centralbank.ie/new-media/press-releases/financialcentres2018-3oct2018](https://www.centralbank.ie/new-media/press-releases/financialcentres2018-3oct2018), accessed 14 Jan 2020.

5 Monetary Authority of Singapore, “Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector” (“FEAT Principles”), 12 November 2018, [https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT](https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT), accessed 14 Jan 2020.
| Principle       | Rationale for Principle | AI Use Case                                                                 | Risk Mitigant                                                                 |
|-----------------|-------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Accountability  | Firms are accountable for both internally developed and externally sourced AIDA models and customers are provided with channels to enquire about, inform, submit appeals for and request reviews of AIDA-driven decisions that affect them. | A customer claim is brought in relation to the mis-selling and incorrect pricing of a financial product and part of the claim alleges that use of AI contributed to the loss. | Track and document the criteria followed when using the AI model in a way that is easily understood and keep a register of the evolution of the models. Ensure there is a means to enable the repetition of the process by which a decision was made, the correct version of the model and data could be used. This may require that the AI model and data will need be recovered from repositories with previous versions of models and data. Make sure the use of AI enablers is traceable through the use of audit logs and establish an audit programme for both the technical design and operation use of AI but also the governance structures that resulted in that use being approved. Make the data, features, algorithms and training methods available for external inspection e.g. by giving the customer a definitive list of data sources and offering clearly illustrated contrastive explanations i.e. generating two contrasting explanations, for example in the form of two opposite feature-ranking diagrams, showing the features that contributed most to that result (with their importance) and the features that least contributed to that result. |
| Transparency    | To increase public confidence, use of AI is proactively disclosed to customers as part of general communication and customers are provided, upon request, clear explanations on what data is used and the consequences of AI decisions made. | A customer complains to a regulator querying how much of the data being used by the bank within its AI solution is being taken from external sources e.g. social media and online interactions and how. | The MAS confirmed that existing risk management models need some refinement to deal with the challenges of AI – enabled innovation. In October 2019, the Basel Committee on Banking Supervision’s (BCBS) Supervision and Implementation Group (SIG) held a workshop on the use of artificial intelligence (AI) and machine learning (ML) in the banking sector which publicly confirmed a view that AI models may amplify traditional model risks for banks. A key area of risk highlighted by participants the quantity and quality of vast data sets, data access and engagement with third parties that use or store data. This also raises the challenge of effective third party vendor management in support of an AI strategy. The European Banking Authority has gone a step further. It considered credit scoring as a clear example of where AI – enabled manipulation of data can deliver real benefits for banks. It highlighted the need to manage legal, conduct and reputation risk but also noted that risk could be higher if external providers are involved in such AI-enabled solutions than it is for services developed in house. It also flagged that ICT change and security risk may possibly increase, as ICT systems would need to develop to be more open to different data sources or technology providers and allow more agility in the use of data. Therefore, the procurement, diligence, negotiation and contract management strategy within organisations should be support any AI innovation strategy. Financial services regulators are promoting principles and giving guidance through public statements to set the expectation that firms need to ensure their governance model is fit for purpose when applied to AI enabled innovation. In time, these regulators will become more proactive in asking firms to demonstrate they fully understand their data assets and to explain how that data is exploited and how the associated risk is mitigated when using AI – enabled technologies. Financial services firms should develop a coherent AI strategy now in a way that anticipates how they will answer that question when it inevitably comes. |

6. **Fibre broadband networks: An investor’s introduction**

By Mike Conradi, Partner, Rubayet Choudhury, Legal Director, and Christian Keogh, Associate, DLA Piper London

Infrastructure and institutional investors are increasingly turning their attention to digital infrastructure assets and the global rollout of fibre broadband. Fibre-to-the-home in particular is seen as an essential component of digital transformation and as providing a large pool of investment opportunities. Though the sector has traditionally been dominated by telecoms players, recent years have seen more interest and deal activity from infrastructure investors and their lenders. Investments can take a number of forms, such as individual projects underpinned by project finance structures and bank debt, or through equity investments in specialist fibre developers. This has led to buoyant M&A activity. Recent examples include:

6 [https://www.bis.org/bcbs/events/191003_sig_tokyo.htm](https://www.bis.org/bcbs/events/191003_sig_tokyo.htm) accessed 14 Jan 2020
• the sale of a 50% stake in Covage (an owner of 45 European networks) by Cube Infrastructure to Altice Europe (which comprises several infrastructure funds managed by AXA Investment Managers, Allianz Capital Partners and OMERS Infrastructure); and
• the sale by TalkTalk of its subsidiary FibreNation (owner of UK networks) to CityFibre (owned by funds managed by Goldman Sachs infrastructure fund and Antin Infrastructure Partners).

All this activity is unsurprising. Infrastructure investors are increasingly categorising this asset class as “core” infrastructure (in the case of PPP deals where payments are paid or guaranteed by government) or, at the very least, as “core+” where there are elements of market risk. Depending on how a project is structured, this asset class could satisfy many of the criteria investors are looking for, such as:

• high barriers to entry;
• long-term and stable returns;
• recognised and established technology; and
• transparent and stable regulatory environments.

Various rollout strategies and business models can be used for the build and rollout of a fibre network. For example:

• a mass residential build v enterprise-focused builds covering metro areas or business parks;
• targeting defined coverage areas where there is less competition v taking a more widespread coverage strategy; and
• a rollout done on an entirely commercial basis v with public support of some kind.

6.1 Key issues for a network rollout

The strategy for network rollout and the inherent characteristics of fibre-to-the-home builds can affect whether an investor can achieve a stable long-term income stream. Here are some of the issues:

• Timing considerations. It takes time to build a fibre network, including building out network coverage to scale to reach more customers. The rollout of a mass residential fibre network can take longer, delaying the provision of access to customers, and also the realisation of investment. On the other hand, a more targeted enterprise build or a business park rollout can be more self-contained, and speed up realisation of your investment. Perhaps easiest of all is to incorporate a fibre build into a new residential or business development.

• 15–20 year payback periods. Fibre networks typically have a lengthy payback period given the high construction costs – perhaps 15–20 years.

• Asset life. The expected useful life of the typical optic fibre asset is as much as 20 years or more. Such a long tenure leads to the possibility that equity investors could seek to maximise the upside after the repayment of bank debt. Though fibre is generally more reliable than the copper alternative, this can still mean that repairs might be needed over time, and it is also likely that significant technology upgrades will be required during the period.

Usually, these upgrades can be achieved without needing major new civil engineering works (because the equipment used to “light” the fibres can be upgraded without the need for work on the fibre) and this should be modelled as part of the overall project costs.

• Market Risk and Subsidies. Depending on the type of rollout, there may be significant market risk – i.e. no assured base of customers for the network after the build is complete – especially if building out a fibre network in areas already covered by incumbent (or other) providers of fibre, where there may be competition. This means that investors will typically have to accept a significant degree of risk when compared with other types of infrastructure asset, such as a power station, where very long-term offtake agreements can be reached.

More targeted fibre network builds – such as rollouts to business parks, new developments or specific enterprise locations like supermarkets and retail sites – may mean more certainty of income after the build is complete. It may be possible in these cases to get large enterprise customers to sign up for at least medium-term contracts as pre-sales in advance, in order to guarantee some income stream that may improve the bankability of a project for lenders. If the build is in a remote or rural area it may also be possible to obtain a public subsidy of some kind – subject to state aid rules – which can mitigate this risk significantly.

• Retail competition among fibre providers is based largely on price. Competition in the retail fibre market is largely commoditised: based on price, and retail prices for the same amount of bandwidth can change, perhaps quite significantly over the life of the asset. Due to long-term payback periods, this can increase the uncertainty of returns. Despite this, the average revenue per user for fibre broadband in Europe has been roughly stable at an average of EUR22 per month over 2011–2018. As technology improves, customers expect greater bandwidths, meaning there will be a need for upgrades to the network infrastructure – but they also appear willing to keep paying a roughly constant amount.

• Technology obsolescence risk and 5G. Fibre is the current gold standard, and the current focus in many markets is on upgrading networks to full fibre (i.e. fibre to the home, from the exchange all the way to the end user’s premises, rather than fibre to a street cabinet and then legacy copper for the last stretch). It seems unlikely that a newer and better technology will be developed in the next 10–20 years to replace it. That said, 5G mobile technology may represent a threat to elements of the retail broadband market.

---

7 Statistica (2019), average revenue per user of fixed broadband in Europe from 2011 to 2018.
8 For example, the UK government has set a goal of achieving full fibre coverage by 2033.
– customers may find they can use 5G instead of a fixed connection to their homes. Although this is a risk to some fibre business models (especially those focusing on the residential market), even 5G will still require much more fibre to be built,\(^9\) albeit to serve multiple 5G base stations rather than homes. It is also possible that the global trend in recent years of rapid increase in demand for fixed bandwidth to homes and offices will mean that even 5G will not be a suitable substitute for a fixed connection (which will likely always be faster and more reliable than wireless ones).

- **Regulatory dynamics.** The regulatory background is critical to a successful investment and investors will need to understand thoroughly both the position and likely changes over time. In the UK, for example, Ofcom has indicated it will, in most areas of the country (those said to be “potentially competitive”), require Openreach to offer a basic “anchor” broadband service at a regulated price. The level of this price and the areas in which it applies could have a significant impact on a competing provider’s business case.

Regulation can also assist with build costs – for example, where an incumbent is obliged to offer access to its ducts and poles at a regulated price, this can mean a new fibre company can build out their network more cost-effectively and quickly. Of course, this also reduces costs for competing networks too, reducing the advantage that would otherwise be obtained by building a new network. In the EU, it may also be possible to take advantage of the (very complex) rules on “co-investment” so as to enter into a partnership with an incumbent operator to build a new fibre network and then have that new network protected from access regulation.

- **Wholesale/retail.** The owners of a fibre network will need to decide whether to offer wholesale or retail services, or both. If they offer retail services they will need to engage a sales and marketing team and invest in customer support. It could be difficult to do this successfully, especially if they’re trying to do so over a large area of the country. Offering wholesale services, on the other hand, can eliminate the need for these elements, and can reduce market risk (especially if combined with a medium-term financial commitment from a retail partner) – but naturally this is likely to mean lower returns overall, because some of the value will be captured by the retailer.

Though some of these features could be new to some investors into the sector, we expect that the increasing sophistication among infrastructure investors coupled with the growing demand for rapid internet speeds to power the digital transformation will mean that an increasing number of infrastructure investors will seek to enter the market or consolidate their existing interests, particularly through M&A transactions.

---

\(^9\) Ciena, 5G Wireless Needs Fibre, and Lots of It

### 7. Huawei and use of high-risk vendors in UK telecoms networks

**By Mike Conradi, Partner and Christian Keogh, Associate, DLA Piper London**

In July 2019, the UK’s Department of Culture, Media and Sport (DCMS) concluded its **Telecoms Supply Chain Review**, aiming to create an evidence-based policy framework for the telecoms supply chain. As part of the review, the National Cyber Security Centre (NCSC) was tasked by DCMS to conduct a review on the use of high-risk vendors (HRVs) in UK telecoms networks.

Last week, on request from the government, the NCSC published technical advice to telecoms operators on their use of equipment from HRVs in the form of Telecoms Security Requirements (TSR). This advice coincided with the government’s announcement that it would put the TSR framework into legislation “at the earliest opportunity” through a comprehensive new telecoms security regime.

The below sets out what you need to know about the NCSC and TSRs, and how the latter are likely to be enforced.

#### 7.1. What is the national cyber security centre?

The NCSC is a government organisation, operational from October 2016 as part of the government’s National Cyber Security Strategy 2016–2020. Its purpose is to be the “authority on the UK’s cyber security environment”, with the role of “sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues.”\(^10\)

After the Telecoms Supply Chain Review, the NCSC carried out a security analysis for the DCMS into potential risks to the telecoms sector arising from changes in the telecoms supply chain and from existing practices employed by UK operators; and into the residual risks to the UK. After a request from the government, the NCSC published non-binding technical advice to telecom operators on their use of equipment from HRVs.

#### 7.2. What are the telecoms security requirements?

The TSRs are a set of guidelines directed at telecoms operators of FTTP (i.e. fixed fibre broadband) and “legacy” fixed access (i.e. copper) networks, and 4G and 5G mobile networks. They set out the NCSC’s recommendations on the use of HRVs in telecoms networks.

The TSRs are designed to mitigate the risks that HRVs present to telecoms networks, and introduce vendor diversity into the telecoms supply chain. The TSRs attempt to do so by identifying what a high-risk vendor is, and by setting out several ways to manage the security risks presented by high-risk vendors:

---

\(^10\) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)
The TSRs set out non-exhaustive criteria that the NCSC applies when identifying vendors as HRVs. These criteria are to be applied by telecoms operators when deciding whether to use a new vendor in their network, though operators are encouraged to engage with the NCSC when making this assessment.

The TSRs introduce suggestions that limit the use of HRVs in telecoms networks, including thresholds on the use of HRVs in telecoms networks, and complete bans on the use of HRVs in certain core parts of telecoms networks. Specifically, these include: bans on the use of HRVs in certain “core” network functions, including general bans applicable to all networks, and specific bans applicable to 4G and 5G networks; bans on equipment from HRVs near sites that are significant to national security or sensitive networks (e.g., those directly relating to the operation of government or any safety-related systems in wider critical national infrastructure); hard caps on the use of HRVs in FTTP and 5G networks (note: these thresholds are not applicable to 4G networks or legacy networks), as follows:

For FTTP and other gigabit and higher capable access networks, a maximum of 35% of premises passed by a network should be served by equipment from an HRV.

For 5G networks, a maximum of 35% of expected network traffic volume on any particular network passing through HRV equipment, and at most 35% of base stations nationally on any network, should be served by equipment from an HRV.

For both FTTP and 5G networks, a maximum of 35% of all the network elements of a particular equipment class in any particular network should be provided by an HRV. In respect of 4G and legacy fixed access (i.e. copper) networks, an expectation that at least two vendors will be used in the access network, with a roughly 50/50 split between vendors in that case (though no hard cap, like the 35% for 5G and FTTP); a cap on the number of HRVs with any amount of equipment in any given network to one HRV; and use of an HRV is subject to there being in place a specific risk-mitigation strategy, designed and overseen by NCSC, relating to that HRV.

Beyond the specific measures noted above, the NCSC notes that for certain network functions, a case-by-case analysis is required to determine what controls are placed on HRVs.

7.3. How will the TSRs be enforced?

The TSRs are formal guidance, setting out the NCSC’s expectations regarding network security. Compliance with the TSRs is currently voluntary, and so their application and implementation is reliant on their adoption by telecoms operators.

The government has, though, proposed to give legislative backing to the TSRs through a comprehensive new telecoms security regime overseen by it and Ofcom. This regime will be introduced “at the earliest opportunity.”11 Until then, the government notes that the UK “expects UK telecoms operators to give due consideration to [the] advice, as they do with all their interactions with the NCSC.”

As such, though at present there is no strong enforcement backing of the TSRs, there is a clear and serious expectation from the government that telecoms operators comply with the guidance from the TSRs.

7.4. Application to the involvement of Huawei in the UK’s 5G network rollout

As part of its review, the NCSC concluded that Huawei would be an HRV under the criteria in the TSRs. The specific reasons for this classification are set out at paragraph 13 of the TSRs. In summary, the NCSC states that:

- Huawei has a large UK market share, and is subject to Chinese law and so could be ordered to act in a way harmful to the UK;
- China has a history of carrying out cyberattacks;
- Huawei’s engineering quality is low; and
- several of Huawei’s entities are subject to restrictions on their ability to trade with the US, which could affect the quality of their products in future.

Due to this classification, there is an expectation that the various restrictions and thresholds in the TSRs will be applied by telecoms operators regarding the use of Huawei as a vendor in their networks.

The TSRs also advise operators whose “Huawei estates” currently exceed the recommended level for an HRV to reduce them as soon as practical.

7.5. Practical application of the TSRs

There are several practical issues arising from the TSRs:

1 Uncertainty as to the practical application of TSRs. It is unclear how certain matters in the TSRs will practically be implemented, including how the 35% threshold will apply in practice in respect of FTTP and 5G networks. For example, what exactly counts as a “network element” of a particular class? We would expect any legislation to clarify this.

2 Dealing with mergers and divestments. After the rules become law, it is unclear how they would be applied when changes happen in the industry. If, for example, an HRV and another vendor merge, does that mean that all legacy equipment from either of them falls into the HRV category? Or all such equipment sold after the merger? What if an HRV hives-off a part of its business, meaning that operators will suddenly find that, in breach of the rules, they have equipment from two HRVs in their network? Again, we hope that the legislation will clarify these issues.

3 Compensation? It is unclear whether any compensation will be offered to cover the costs of removing HRV equipment. The most likely scenario is that no such compensation will be offered. In that case, foreign investors in UK network companies should consider whether they would have a claim under any relevant Investment Protection Treaties. This could be an option if the government changes the law to require significant new expendi-

11 https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei
ture that applies disproportionately to foreign-owned networks.

4 Application to telco operators. The NCSC’s TSRs recommend that operators whose Huawei “estates” exceed the recommended thresholds reduce them as soon as practical. It is unclear what the NCSC’s advice is on removing the presence of other HRVs from telecoms networks where that presence would fall foul of the new TSR thresholds.