Privacy + Security Forum:

Beyond DPAs: Trends in M&A and Other Data-Driven Transactions

Jay Donde, Senior Corporate Counsel, Privacy @ Salesforce
Christine Lyon, Partner and Global Co-Head of Data Privacy and Security @ Freshfields Bruckhaus Deringer

September 2021

Introduction

Companies planning M&A or other data-driven transactions need to stay informed of evolving data protection requirements that may affect business models. For example, China's recent expansions of its data localization and cross-border data transfer rules require greater attention in assesssing businesses that operate in China, while evolving AI and IoT guidance in the EU signal new directions in assessing AI and IoT businesses. The following updates from Freshfields provide more information about these developments.

Contents

China's restrictions on cross-border data transfer

With the entry into effect of the Data Security Law (***DSL***) and the Regulations on the Security Protection of Critical Information Infrastructure (the ***CII Regulations***) on 1 September 2021, as well as the recent passing of the Personal Information Protection Law (***PIPL***), which will come into effect on 1 November 2021, now is a good opportunity to review all of the non-sectoral restrictions on exports of data from China.

Critical information infrastructure operators

Article 37 of the Cyber Security Law (***CSL***) requires operators of critical information infrastructure (***CIIOs***) that collect either personal data or 'important data' in China to store that data within China. Neither type of data can be transferred overseas without prior regulatory approval having undergone a security assessment, and subject also to demonstrating a genuine business need. Article 37 provides that the rules for conducting the security assessment are to be jointly formulated by the Cybersecurity Administration (***CSA***) and the "*relevant departments of the State Council*". However, despite the CSL having been effective since June 2017, no procedure for obtaining approval and no standards for the security assessment have ever been implemented.

The CSL does not define critical information infrastructure (***CII***), and this category of information network has never been comprehensively detailed since. Indeed, until the recent promulgation of the CII Regulations there had been no definitive statement as to what constitutes CII. In the meantime, it is understood anecdotally that the various Chinese cyber security agencies and sectoral regulators have been advising CIIOs of their status for the past several years based on individual determinations (a practice confirmed by Article 20 of the *Measures for Cybersecurity Review*, which took effect in June 2020).

Article 31 of the CSL adopted the generalised description of CII from the CSA's Cyberspace Security Strategy from December 2016; namely that CII is "*information infrastructure that affects national security, the national economy and people's livelihoods, such that, if data is leaked, damaged or loses its functionality, national security and public interests may be seriously harmed*".

From the National Information Security Standardisation Technical Committee[1] (***TC 260***)'s Method of Boundary Identification for Critical Information Infrastructure issued in August 2020 and Article 9 of the CII Regulations, among other sources, it is possible to extract a non-exhaustive list of industry sectors and business areas that may be liable to be categorised as CII:

- finance
- cloud computing, big data and other large-scale public information network services, including those provided over the Internet
- energy, transportation, water management, sanitation and healthcare, education, environmental protection and public utilities, etc
- scientific research and production in fields such as national defence, industrial equipment, industrial chemicals, food and drugs
- public telecommunications, radio and television stations and news agencies.

[1] TC260 is jointly operated by the CAC and the Standardisation Administration of China.

Article 2 of the CII Regulations states that if an incident affecting an information network within any of these industries and fields may "*seriously endanger national security, the national economy, the people's livelihood and the public interest*" then that network could be deemed to be CII.

Article 9 of the CII Regulations provides that the following factors should be taken into account in the identification of CII:

- the importance of the network, etc., to the relevant industry and its key businesses
- the degree of harm that may be caused by the destruction of the network, or by a loss of functions or data
- the impact of an incident on other industries and fields.

The CII Regulations now formally delegate responsibility for formulating rules for the identification of CII and for making determinations of CIIO status to individual sectoral regulators and responsible government departments, acting under the supervision of the CSA (Articles 9 - 11). It nevertheless remains to be seen whether any precise classification system for CII will be made public any time in the near future.

Article 40 of the PIPL confirms the requirement in Article 37 of the CSL for CIIOs to store personal data inside of China and to undergo a security assessment organised by the CSA before transferring that data overseas. The PIPL leaves many questions unanswered in this respect, such as what the duration of any approval would be and how frequently, or in what circumstances, the security assessment would need to be repeated.

A June 2019 draft of the *Security Assessment Measures* (which was never brought into effect) would have provided that a security assessment is required every two years or when there is a change in the type of personal data being transferred, the purpose of processing or the retention period. A separate approval would be needed to transfer to different overseas recipients but not for a repeated transfer to the same recipient.

The CSL also did not define the concept of 'important data'. However, this category of data has now been elaborated upon in the DSL (which will be discussed further below).

Other organisations

Under Article 38 of the PIPL, organisations that are not CIIOs will be permitted to transfer personal data out of the PRC where "*necessary*", up to a certain threshold level (to be specified at a later date) by either:

- entering into a standard form CSA data transfer agreement
- obtaining a personal data protection certification (likely to be akin to the GDPR's 'binding corporate rules' – the CSA will publish regulations in due course)
- passing the same CSA security assessment that will apply to personal data transfers by CIIOs.

Article 38 of the PIPL does appear to indicate that the PRC authorities will give effect to cross-border data transfer mechanisms in international treaties and agreements that China is a signatory to. This would include the Cross-Border Privacy Rules (CBPR) system of data privacy certifications implementing the APEC privacy framework. However, this provision of the PIPL will need clarification.

Organisations exporting personal data will also be responsible for taking all necessary measures to ensure that overseas recipients provide a standard of protection for the transferred personal data that is consistent with the requirements of the PIPL and to ensure that the data is only processed within the scope and for the purpose consented to (Articles 21, 23 and 38).

Transfers of personal data above the specified threshold will also be required to pass the same security assessment (Article 40). It remains to be seen whether the threshold will be a straight annual volume threshold or whether additional sub-thresholds will be applied to individual transfers or to transfers of data of a certain type, e.g. sensitive personal data.

Similar to the CSL, Article 39 of the PIPL requires organisations transferring personal data out of China to inform individuals of:

- the type of personal data that will be transferred
- the name and contact information of the overseas recipient
- the reason for the transfer

- how the overseas recipient will process the data
- the channels for the individual to exercise his or her individual data subject rights as against the overseas recipient[2].

The individual's specific consent must also be obtained to transfer their personal data out of China. And this consent must be explicit, voluntary and fully informed (Article 14). Fresh consent will need to be obtained if the purpose or method of processing is changed.

For other data processing activities, the PIPL departs from the solely consent-based approach of the CSL, enabling personal data to, for example, now also be processed where necessary for the conclusion or performance of a contract, or if the data is already in the public domain, in which case the data can be processed within a "*reasonable scope*" (Article 13).

The law does not elaborate on the minimum provisions of a data transfer agreement and the CSA has yet to release a draft of the standard form data export agreement referred to in Article 38. The requirements for data export agreements were, however, set out in some detail in the June 2019 draft of the *Security Assessment Measures* and followed at that time the outline of the EU's standard contractual clauses.

There are no exceptions for transfers to an overseas affiliate. Moreover, in a set of draft guidelines issued in 2017 (the draft *Guidelines for Cross-Border Data Transfer*), cross-border transfers were defined to include remote access from overseas.

Under the PIPL, organisations will further be required to conduct a specific data protection impact assessment (***DPIA***) before undertaking a data export. The risk assessment should consider:

- whether the purpose and method of processing are legal, legitimate, and necessary
- the impact on individuals' rights and interests
- the risk level and whether the security measures taken are commensurate to the level of risk.

The written DPIA will have to be kept for at least three years, but will not need to be submitted to the authorities.

Third party processors will be required to return or delete personal data after the engagement ends, and may not appoint sub-processors without approval (Article 21).

Important data

Article 31 of DSL confirms the requirement laid down in Article 37 of the CSL for CIIOs to store 'important data' locally. Rules for exports of 'important data' by non-CIIOs will be formulated by the CSA and other authorities of the State Council at a later date.

The DSL does not, however, define 'important data'. Article 21 of the DSL states only that regional and sectoral regulators will be tasked with formulating specific catalogues of 'important data' for their respective sectors in line with a yet-to-be-developed national classification system - "*based on the importance of data in economic and social development and the degree of harm that would be caused by its destruction, divulgence, illegal acquisition or utilisation, or being tampered with, to national security, the public interest or the lawful rights and interests of individuals and organisations*".

Core national data that is significant for national security, the national economy, people's livelihood or material public interests will be subject to a more stringent management system, the details of which are yet to be made public.

The draft *Measures on the Management of Data Security* issued in 2019 referred to 'important data' as data that would directly impact national security, economic security, social stability or public health and security if leaked. A catalogue contained in the draft *Guidelines for Cross-Border Data Transfer* in 2017 indicated that 'important data' could include statistical and other aggregated data sets of economic information. Neither of these drafts were ever brought into effect, however.

---

2 Namely the right to object to processing, right of access and correction, right of data portability and right of erasure (Chapter IV, PIPL).

Review Measures

In early July 2021, the CSA announced cyber security inspections into Didi Chuxing, which operates the popular ride-hailing app 'Didi', Full Truck Alliance (FTA), which operates two truck-hailing apps, and Kanzhun, which operates the 'Boss Zhipin' recruiting app. The grounds for these investigations have not been made public but came within weeks (or days in the case of Didi Chuxing) of each of these companies having completed their initial public offerings in the United States.

Shortly afterwards, the CSA conducted on-site inspections together with seven other regulatory authorities, including the Ministry of Public Security and the State Administration for Market Regulation (SAMR) pursuant to the Measures for Cybersecurity Review issued in June 2020 by (the ***Review Measures***). The Review Measures set out a procedure for national security review of CIIOs when purchasing network products and services that may impact national security. See earlier briefing here.

On 10 July 2021, the CSA published a consultation draft of a revision to the Review Measures that proposed to expand the ambit of the review to encompass, in addition to CIIOs, organisations that hold the personal data of more than a million users and which intend to pursue an overseas listing (anywhere other than in Hong Kong), among other new grounds. The potential security risks to be assessed are also proposed to be expanded to include the risk that: (i) 'core data' or "*large amounts of personal data*" may be illegally exported or used; and that (ii) after an overseas listing, 'core data', 'important data', or large amounts of personal data could become controlled or used maliciously by a foreign government.

Provision of data to overseas regulatory authorities

Both the PIPL (Article 41) and DSL (Article 36) provide that organisations in the PRC may not disclose to a foreign judicial or law enforcement body any information (personal data in the case of the PIPL, and any data in the case of the DSL) that is stored in China without approval from the competent authorities. The assessment of requests for cooperation by overseas judicial and law enforcement bodies is to be based on "*principles of equality and reciprocity*" (Article 36, DSL).

The EU's proposed AI Regulation

What you need to know

Technological advances in the field of artificial intelligence have brought about sweeping economic and societal benefits, with an exponential boom in the development and deployment of AI systems across sectors. AI sits at the heart of the global trend towards digitalisation and its various applications have huge potential to improve the ways in which businesses run and in which we, as consumers, interact with them and with each other.

However, with new technological benefits come risks and regulation. On 21 April 2021, the European Commission published its draft legislative proposal on artificial intelligence (the ***AI Regulation***). The AI Regulation attempts to strike a balance between addressing perceived risks linked to AI, on the one hand, and not unduly constraining or hindering technological development or otherwise increasing the cost of placing AI solutions on the market, on the other. Some commentators have already suggested that it is more successful at the former than the latter.

Although the AI Regulation will not come into force until it has passed through the European legislative process, the significant regulatory requirements in the proposed text cannot be ignored. The AI Regulation will play a key role in shaping how AI is developed in the EU and will likely also serve as a blueprint for other regulatory authorities around the world contemplating similar regulation. It could also provide another opportunity to test the new and emerging relationship between the EU and the US on technology and data issues.

The AI Regulation encompasses a wide-ranging set of rules seeking to regulate the pervasive use of AI across a spectrum of industries and social activities, with rule breakers facing the possibility of fines of up to 6% of global turnover. It is a culmination of three years of work, during which the Commission undertook extensive consultations with industry and wider society, receiving more than 1,200 responses worldwide on its February 2020 White Paper alone.

At its core, the AI Regulation proposes a sliding scale of rules based on risk: the higher the perceived risk, the stricter the rule. This, the Commission believes, will allow legal intervention to be tailored to those situations where it thinks there is justified cause for concern or where such concern can reasonably be anticipated in the near future.

We outline below which businesses are affected by the AI Regulation, what they need to know and how they should be approaching compliance in the future.

Who and what is subject to the AI Regulation?

The AI Regulation has a wide reach:

Actors. The AI Regulation will apply to various participants across the AI value chain, covering both public and private actors inside and outside the EU as long as the AI system is placed on the EU market or the output produced by the system (such as content, predictions, recommendations, or decisions) is in the EU. Strict requirements may apply inter alia to providers, users, end-product manufacturers, importers or distributors, depending on the risk associated with the AI system.

Broad-brush definition of AI. An AI system is defined as software that is developed with machine learning, logic- and knowledge-based or statistical approaches which can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

The remit of the AI Regulation goes beyond modern machine learning systems that learn to make decisions themselves, also capturing systems that operate according to hard coded rules, which have long been embedded in a wide variety of applications (from flight control to pacemakers to industrial settings). The Commission's expansive approach means virtually all systems that currently do, or which may in future, use AI would fall within scope – from personalised pricing, advertising and feed algorithms, to

connected IoT systems, self-driving cars, or applications used to support recruitment and other business processes.

A sliding scale based on risk

The AI Regulation focuses on when, where and how AI is developed, marketed, and used. Every application and use case of AI will fall into one of four different risk categories: **unacceptable**, **high**, **limited** and **minimal**, with differing degrees of regulation applying to each. The higher the risk, the stricter the requirements.

The AI Regulation also contains future-proofing provisions allowing for additions and/or expansions to these categories, and the examples contained within them, to cover emerging uses and applications of AI.

"Unacceptable risk" – prohibited

There is an outright prohibition on certain AI systems which the Commission deems to pose an unacceptable level of risk, i.e. which are assumed to be particularly harmful and to contradict values of respect for human dignity, freedom, equality, democracy and the rule of law and EU fundamental rights. This is an exhaustive list which, in summary, focuses on:

- AI systems that distort human behaviour in a manner causing physical or psychological harm by deploying subliminal techniques or by exploiting vulnerabilities due to the person's age or physical or mental disability.
- AI-based social scoring systems deployed by public authorities leading to the detriment of individuals or groups of people.
- AI systems used for real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement, subject to a number of exceptions.

While the latter two categories are focussed on public authorities and law enforcement, the first category is more relevant to private actors' own interactions with end-users. Certain AI applications could be said to involve "deploying subliminal techniques" to influence human behaviour. The limiting factor set by the AI Regulation is the causation of physical or psychological harm, but this is not explicitly defined in the regulation. If that remains the case in the final regulation, what amounts to psychological harm may be a key battleground in any future AI disputes.

"High-risk" – strictly regulated

High-risk AI systems are those which affect human health and safety, or which involve the use of intrusive data analytics and profiling that could affect fundamental rights. Such systems will need to undergo a conformity assessment procedure to verify that they comply with a set of specifically designed high-risk requirements (explained below), following which a written declaration of conformity must be drawn up, a CE mark applied and the AI system registered in a new EU database to be set up by the Commission.

High-risk AI systems are split into two categories:

1. *Safety products/components*. This covers AI systems which are used as safety components in products (or are themselves products) that are already subject to existing conformity assessment systems under specific EU harmonisation legislation. For example, existing EU regulations require cars, medical devices and industrial machinery to be assessed for conformity with various essential safety requirements before they can be placed on the market. Once the AI Regulation comes into force (along with any relevant secondary legislation, e.g. implementing acts specific to automated vehicles), these existing conformity assessments will also include compliance with the high-risk requirements described below. This would cover, for example, the use of machine learning in an autonomous vehicle or an AI-enabled pacemaker.
2. *Specific uses of AI in sensitive sectors with fundamental rights implications.* This covers AI systems which are not used in situations that are already subject to EU harmonisation legislation, as above, and which fall into one of eight areas listed in Annex 3 to the regulation.

High-risk applications (Annex 3)

1. AI used for **biometric identification and categorisation of natural persons**
2. AI used as safety components in the **management and operation of critical infrastructure**, **such as the supply of utilities**
3. AI used for determining access to, and assessments in, **educational and vocational training**
4. AI used in **employment**, **workers management and access to self-employment**, including the use in recruitment, task allocation or monitoring and evaluating performance
5. AI used to evaluate the creditworthiness of individuals or their credit score, or in certain other manners that determines **access to and enjoyment of essential private services and public services and benefits**
6. AI used in **law enforcement** for individual risk assessments or as polygraphs
7. AI used for assessing security risks in **migration**, **asylum and border control management**
8. AI used to assist a judicial authority in the **administration of justice and democratic processes**

Products or services which fall into these use cases will be subject to self-assessment conformity obligations to confirm compliance with the high-risk requirements described below, with the exception of systems for biometric identification and categorisation of natural persons, which will be subject to conformity assessment by an external testing body.

Because these high-risk requirements are wide-ranging (see below), conformity assessments of any kind will impose significant burdens on those who develop, market or use AI applications falling into either category. The impact may vary by sector and use case. Systems for the management of critical infrastructure are already tightly regulated and controlled, and those responsible for them will be used to operating within a complex regulatory framework. In contrast, providers and users of biometric scanners or recruitment software may find these changes more demanding. The AI Regulation seems particularly keen to tighten protections around algorithmic bias and discrimination in the work place, and performance management algorithms – such as those found to be discriminatory to certain categories of riders in a recent ruling by an Italian tribunal concerning an algorithm used by a food delivery platform – would be treated as high-risk applications.

At the same time, AI developers will welcome the Commission's stance that only self-assessment conformity is required for most high-risk AI systems, saving them from having to disclose their algorithms and underlying training data to external testing bodies for review, thereby ensuring that intellectual property protections and trade secrets for those assets are not compromised.

"Limited risk" – enhanced transparency

The AI Regulation identifies three categories of AI systems which, while not necessarily "high-risk", will need to fulfil requirements in terms of transparency:

1. AI systems that interact with natural persons will need to be designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and context.
2. Emotion recognition or biometric categorisation systems must inform end-users that they are exposed to such a system.

3. AI systems that generate or manipulate content to resemble existing persons, objects, places or other entities or events, so that the content would falsely appear to a person to be authentic (i.e. a 'deep fake'), must disclose that the content has been artificially generated or manipulated.

These applications do not, however, need to comply with the high-risk requirements (below) or undergo conformity assessment, unless they separately constitute high-risk applications (e.g. an AI system with which employees interact in order to obtain access to vocational training).

"Minimal risk" – no additional restrictions

The EU expects that the "vast majority" of AI technology will fall into the minimal-risk category, which is free to develop and use with no restrictions on top of any relevant existing legislation (this category is not formally listed in the legislative proposal but is detailed in the Commission's Q&As published alongside the proposed AI Regulation). No conformity assessment is required for such technology. Examples would include email spam filters and mapping products used for route planning.

At the same time, the Commission and the newly formed European Artificial Intelligence Board (see below) will encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application of the mandatory requirements for high-risk AI systems even for those AI systems that do not fall within the high-risk category.

High-risk requirements

High-risk AI systems must comply with several mandatory requirements before the system can be placed on the market or put into service, or before its output can be used in the EU. Conformity assessment (as described above) is intended to certify that the system in question meets these requirements:

1. **Risk management systems** must be established, implemented, documented, maintained and regularly updated. The risk management system must identify and analyse foreseeable risks associated with the AI and eliminate or reduce those risks to the extent possible and otherwise implement control measures in relation to those risks.
2. **Data and data governance**. High-risk AI systems which involve training models with data must use training, validation and testing data sets which are subject to appropriate data governance and management practices, are relevant, representative, free of errors and complete, and take into account the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the AI system is intended to be used.
3. **Technical documentation**, containing as a minimum the information detailed in Annex IV, including a detailed description of the elements of the AI system and the process of its development, must be drawn up before the AI systems are placed on the market or put into service, and must be kept up-to-date.
4. **Record keeping**. High-risk AI systems must have logging capabilities ensuring traceability of the AI system's functioning throughout its lifecycle, at a level appropriate to its intended purpose.
5. **Transparency and provision of information to users**. The operation of high-risk AI systems must be (i) sufficiently transparent to enable users to interpret the AI system's output and use it appropriately; and (ii) accompanied by instructions for use, including any known and foreseeable circumstances that may lead to risks to health and safety or fundamental rights, human oversight measures, and the expected lifetime of the high-risk AI system. The information must be concise, complete, correct and clear, and must be relevant, accessible and comprehensible to users.
6. **Human oversight**. High-risk AI systems must be capable of being overseen by natural persons, with the aim of preventing or minimising risks to health, safety or fundamental rights. The provider is to identify and build (where possible) oversight measures into the AI system. The designated individual should fully understand the capacities and limitations of the AI system and be able to monitor its operation and output for signs of anomalies,

dysfunctions and unexpected performance. Humans should be able to intervene and stop the system.

7. **Accuracy, robustness and cybersecurity**. High-risk AI systems must, in light of their intended purpose, be appropriately accurate, and the accuracy metrics must be declared in the accompanying instructions of use. The systems must also be appropriately robust and resilient to errors, faults or inconsistencies and resilient to third parties intending to exploit system vulnerabilities, including data poisoning and adversarial examples.

These high-risk requirements will be onerous to comply with. Potential issues include:

- The requirement that data sets be "representative" does not sit easily with GDPR requirements regarding sensitive personal data. Similarly, a provider of a high-risk AI system is allowed to process the GDPR special categories of personal data for the purposes of ensuring bias monitoring, detection and correction in those systems, subject to certain safeguards. But minimal detail is provided as to what those safeguards would encompass.
- The requirement that data used to train AI systems be "free of errors and complete" may well be unachievable in practice, given the scale of the data sets used in machine learning.
- The requirement, in certain circumstances, for a designated individual to be able to "fully understand" the operation of a complex AI system, sets a very high bar; this is unlikely to be an attractive role for anyone to take on.
- Traceability requirements may pose problems for certain deep learning AI systems, where it is difficult to clearly explain and trace how the system is functioning.

On whom do these obligations fall?

A **Provider** is anyone who develops an AI system, or has it developed with a view to putting it on the market or into service under its own name or trademark. Providers of high-risk AI systems have primary responsibility for ensuring compliance with the AI Regulation. They must:

- ensure that the AI system complies with the high-risk requirements
- manage the conformity assessment procedures and inform national competent authorities of any non-compliance
- put in place a post-market monitoring system to collect, document and analyse data throughout the lifetime of the AI system and to evaluate the AI system's continuous compliance
- a third party will also be treated as a provider if, for example, it places on the market or puts into service an AI-enabled product under its own name or brand, or makes a substantial modification to an existing high-risk AI system

A **User** is anyone deploying an AI system under its authority, but does not include personal and non-professional uses (e.g. everyday consumers). Users have more limited obligations than providers, but still have various monitoring and information obligations:

- use the AI systems in accordance with the instructions of use
- ensure that input data is relevant in view of the intended purpose of the AI system
- monitor the operation of the AI system on the basis of the instructions of use
- inform the provider or distributor of any risk to health and safety or fundamental rights
- keep automatically generated logs to the extent that such logs are under their control

Manufacturers of products which are already regulated under EU sectoral legislation (cars, medical devices etc) and which use high-risk AI, are subject to the same obligations as providers. There are also obligations on **importers** and **distributors** of high-risk AI systems.

Governance and penalties

The AI Regulation proposes the establishment of a new European Artificial Intelligence Board composed of representatives from the Member States and the Commission to assist with implementation. Its intended role seems to be similar to that of the European Data Protection Board (EDPB), as regards GDPR.

The AI Regulation provides for a significant set of tiered fines:

1. **30m EUR or 6% of total worldwide annual turnover** for non-compliance with the prohibition on unacceptable-risk AI systems or the data governance requirements.
2. **20m EUR or up to 4% of total worldwide annual turnover** for supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities, in reply to a request.
3. **20m EUR or up to 4% of total worldwide annual turnover** for supply of incorrect, incomplete or misleading information to notified bodies/national competent authorities, in reply to a request.

Looking ahead

The AI Regulation will apply (with limited exceptions) to AI systems that are placed on the market, put into service, or high-risk AI systems that have significantly changed, two years after the AI Regulation enters into force. An AI system's inherent adaptation on the basis of its machine learning application does not constitute significant change.

However, the AI Regulation is still a draft, and it will need to pass through the European legislative process – this includes a review by the European Parliament, which has previously voiced the need for broad regulation, as well as the Member States. Given the degree of interest shown in the AI Regulation even before its publication, that legislative process is likely to be protracted. We expect inter-institutional negotiations to finalise the text will take between 18 and 24 months, and the regulation could theoretically apply as from early/mid 2024.

We expect considerable debate in the European Parliament as to which committee takes the lead on the proposal, given that many have prepared reports to guide the future legislation. MEPs are likely to seek to toughen the proposal, including likely pushback on the exceptions provided to law enforcement to deploy prohibited uses and the fact that quality management and conformity assessment procedures are only needed for high-risk AI systems. In addition, there is broad scepticism with regard to the creation of another body (the European Artificial Intelligence Board) that could wield material power in deciding what gets added to or taken out of the high-risk and the prohibitions lists (especially when many consider that the European Data Protection Board could perform this function).

Beyond the AI Regulation, wide-ranging though it is, the EU is also considering how other aspects of emerging technologies such as AI should be regulated. For example, it remains to be seen whether proposals will follow to amend the rules governing businesses' liability to consumers for harm caused by AI-enabled products.

What are the top points I should be thinking of today if...

I'm a provider or user of AI

1. Get ready for the new regulation by assessing the likely impact of the proposal on your business and by developing mature AI governance frameworks.

2. Engage with the EU institutions as the proposed regulation is examined and amended: the AI Regulation is still at an early stage of the legislative process and it is likely that Member States in Council and MEPs will be actively seeking input from stakeholders. This could be done individually, or via trade associations, a number of which have already been actively working on the Commission's AI work streams. These include DIGITALEUROPE, DOT Europe, MedTech Europe, EuroCommerce and AmCham EU, to name a few.

3. Monitor the development of this regulation, and related changes in areas such as liability, in the months ahead.

I'm investing in AI

1. .Assess which risk category any target AI systems would fall into and whether there is a risk that these systems shift between risk categories with future technological advances or regulatory

2. Understand the extent to which a target business complies (or can easily be made compliant) with likely future regulatory requirements, in the same way that preparedness for GDPR was assessed in the past. Consider, in particular, whether AI systems are so deeply integrated into applications that they will be difficult to adapt to fit with future regulation.

3. The EU believes development and commercialisation of AI will be driven by public trust. Assess whether the target is at a level where it could promote and explain the trustworthiness of its AI.

4. Diligence whether any target AI systems are built on third party component AI systems, models or datasets – and test whether the business has appropriate licences to use them.

5. Consider the global direction of regulatory travel: assess where the target operates its AI systems and consider whether other jurisdictions will pass similarly strict regulation. EU officials say Japan and Canada are already taking a close look at its proposal.

Germany's new ePrivacy requirements: big challenges for the IoT space

With very little media attention, the German parliament has passed the Telecommunications and Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutz-Gesetz* – TTDSG), which will come into force on **1 December 2021**.

The TTDSG, among other things:

- combines the data privacy provisions of Germany's Telecommunications Act (TKG) and the Telemedia Act (TMG); and
- finally transposes Article 5(3) of Directive 2002/58/EC, as amended by Directive 2009/136/EC (known as the 'ePrivacy Directive' or 'Cookie Directive') into national law.

The TTDSG aims to be Germany's comprehensive ePrivacy legislation for communication and online services, way before the EU ePrivacy Regulation – for which the legislative process is likely to drag on for several years – comes into force.

Key aspects

The main aspects of the TTDSG are as follows:

- The TTDSG applies to almost every device with an internet connection, such as smart-phones, computers, smart-TVs and other internet-of-things (IoT) devices (especially smart-home devices such as security cameras, lights and speakers) and connected vehicles.
- The new legislation covers, among other things, telecommunications secrecy and wiretapping bans, traffic and location data, regulations on itemised bills and billing, incoming calls, caller-ID display and suppression, telephone directories, and, in the case of telemedia providers, technical and organisational measures, the processing of data relating to minors, and obligations to provide information on inventory and usage data and passwords.
- The core of the new TTDSG is section 25, which regulates the protection of privacy in devices and requires – in principle – end-users to consent to any storage of and access to (**non-personal**) information stored in their devices. This affects all IoT service providers who in some form or another access data on users' devices.
- Consent is always required, unless the sole purpose of the storage or access is the execution of the transmission of a message via a public telecommunications network or if the storage and access is needed to provide a telemedia service requested by the user. It is unclear whether legal obligations which require access to a device (e.g. product safety monitoring obligations) create an exemption from the consent requirement under the TTDSG.
- The competent supervisory authority can impose fines of up to €300,000 per case for violations of the TTDSG. If applicable, GDPR fines may be imposed on top (see more below).

How the TTDSG works with the GDPR

The EU General Data Protection Regulation (GDPR) will still apply in addition to the TTDSG. In a nutshell, the TTDSG has some form of gatekeeper functionality and imposes requirements on accessing a device via the internet, whereas the GDPR sets out requirements on processing personal data by this access. The TTDSG, however, imposes additional obligations to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union as set out set out in Directive 2002/58/EC.

Taking action

The IoT space and all other business that rely on accessing data on user devices have very little time to prepare for the requirements of the TTDSG.

Under the new law, data storage and access on a device will face much more scrutiny and may no longer be viable unless it falls under the narrow legal exemptions or users give their consent (a process that could be quite complicated).

This will particularly be the case where use-cases previously relied on the controllers' legitimate interest. All use-cases should therefore be reviewed in order to determine if they need changing. While doing so, the following aspects must be considered.

Accessing a device via a telecommunication network

The consent requirement only applies to access via the internet, which applies to all IoT devices. For connected vehicles, the European Data Protection Board mentioned in its 2020 guidelines on processing personal data in the context of connected vehicles and mobility-related applications that a connected vehicle and every device connected to it is considered 'terminal equipment' under the ePrivacy Directive and therefore the TTDSG.

Providing a telecommunication or telemedia service

Depending on the nature of the telecommunication or telemedia service provided, a legal exemption might apply. If so, this should be documented. With the accompanying amendments to telecommunication law (*Telekommunikationsmodernisierungsgesetz* – TKMoG), which will also come into force on 1 December 2021, further requirements, in particular slightly amended definitions, should be considered.

Introducing a consent-management system

If no legal exemption applies, data storage in the device (ie updates) and access to data already stored in device requires consent, which must be provided in compliance with the GDPR. This may require a new consent-management system for use-cases that previously relied on legitimate interest.

Competent supervisory authority

Depending on the nature of the service, the competent supervisory authority could be the Federal Commissioner for Data Protection and Information Security (*Bundesbeauftragter für Datenschutz und Informationssicherheit*), the relevant state data protection authority (*Landesdatenschutzbehörden*) or even the Federal Network Agency (*Bundesnetzagentur*).