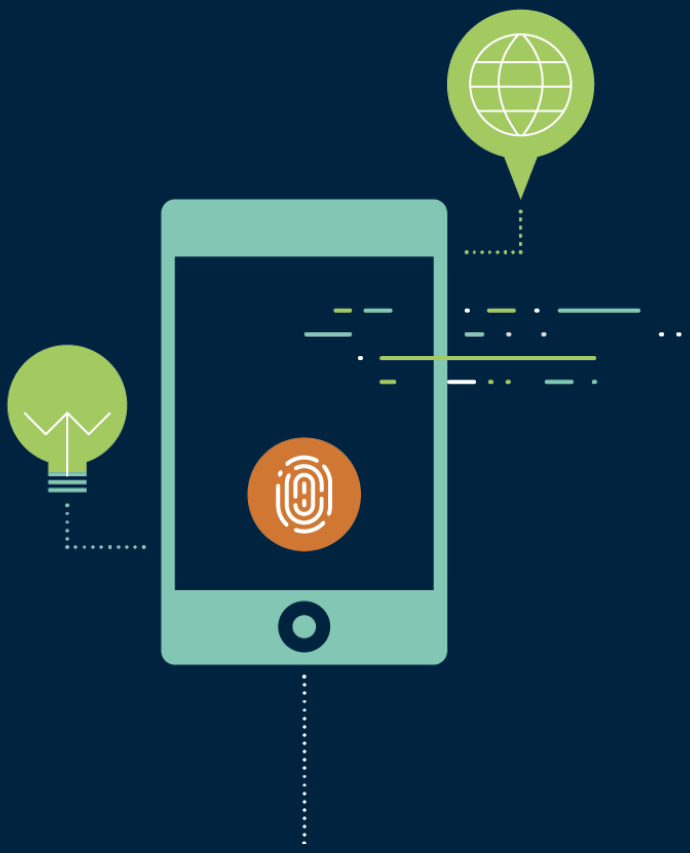
TRAVERS SMITH

Data and the digital economy – current data issues

December 2020



traverssmith.com

Overview

Modern digital economies are powered by data, which is now a significant economic asset in its own right. In the UK's recently published National Data Strategy data was described as a 'geostrategic tool'.

In 2016 the McKinsey Global Institute estimated that, in 2014 the international flow of data added US$2.8 trillion to the global economy and this was expected to grow to US$11 trillion by 2025.

International data flows in a new world order: webinar

In a webinar hosted by Travers Smith on 24 November 2020 we examined the rules around privacy and data protection in the context of international data flows, Brexit, and the perspective from the US.

Our speakers were Nicky Morgan, former Digital Secretary, now a consultant at Travers Smith; Sabina Ciofu, Head of EU and Trade Policy at techUK; Richard Ward, Global and Regulatory Affairs at IBM and Chair of techUK's Data Protection Committee; Dan Reavill, Head of Commercial, IP and Technology at Travers Smith and Jeannie S. Rhee, Partner and specialist in data innovation, privacy and cyber security at Paul, Weiss, Rifkind, Wharton & Garrison LLP.

In particular we looked at the move by some governments and institutions towards protectionism with regards to data, the way that this has manifested itself in relation to transfers of personal data from the EU and the difficulties this has caused for businesses which rely on data flows, especially in light of Brexit, for UK based businesses and their EU counterparts.

This briefing sets out the points that were made, together with a number of other notable developments in relation to data. These developments help to underline the increasing importance that data is playing in the economy and the world.

Cross border digital trade

In the UK all eyes are on the Brexit negotiations to see if the UK will be granted equivalence with the EU's data protection regime. Although the UK's current regime is clearly equivalent to and compliant with the General Data Protection Regulation 2016/679 (GDPR), the EU is wary of any changes the UK might make post Brexit to its data protection regime.

The UK's stated intention is to obtain a decision from the EU that the UK's current data protection regime is deemed to be 'adequate' to allow the continued free flow of personal data between the UK and EEA. However, as with financial services, the adequacy decision is part of the wider political negotiations and so has not yet been granted even though it could be treated separately.

Given current timings, we can expect an announcement by mid-December, although the question of whether any adequacy decision comes with or without strings attached (for example in relation to onward transfers of personal data about EU data subjects), remains to be seen. It is also important to remember that any decision that is granted, won't be insusceptible to challenge, as we saw earlier this year in relation to the EU-US Privacy Shield.

As part of the 'no-deal' preparations companies are being encouraged to include Standard Contractual Clauses (SCCs) in relevant agreements relating to the transfer of personal data in case the adequacy decision is not made before 1 January 2021 (please see below for further details about this).

The EU's stance towards the UK on equivalence will be of interest to other countries hoping to negotiate trade agreements with both the EU and, in future, with the UK.

The flow of data will be an important component in the UK's trade agreements with other countries too. The UK/Japan agreement, the outline of which was published in September 2020 is said to include:

"Cutting-edge digital & data provisions that go far beyond the EU-Japan deal. These will enable free flow of data whilst maintaining high standards of protection for personal data. We have also committed to uphold the principles of net neutrality, as well as introducing a ban on data localisation, which will prevent British businesses from having the extra cost of setting up servers in Japan."

The UK has agreed a roll-over with Canada of the EU's CETA agreement and is said to be close to reaching agreements on trade with Australia. In the case of Australia the UK's stated strategic aim is to "include provisions that facilitate the free flow of data, whilst ensuring that the UK's high standards of personal data protection are maintained and include provisions to prevent unjustified data localisation requirements."

Transfers of personal data from the EEA

One of the significant data protection developments of the year, was the judgment of the Court of Justice of the European Union (CJEU) in Schrems II[1] , which not only invalidated the EU-US Privacy Shield as a mechanism for transferring personal data from the EEA to the US, but also set out further guidance for data exporters and importers to follow when relying on SCCs as the appropriate GDPR mandated safeguard for transferring personal data to third countries. The judgment reminded data exporters that the protection granted to personal data in the EEA, must travel with the data wherever it goes, and that controllers, when exporting data, are responsible for verifying on a case by case basis, and where appropriate, in collaboration with the importer in the third country, if the law or practice of that country impinges on the effectiveness of SCCs to ensure contractually, an essentially equivalent level of protection for the data which is the subject of the transfer.

European Data Protection Board (EDPB) Guidance

The judgment has now been supplemented by the eagerly awaited draft guidance of the EDPB (which is made up in part of the heads of data protection supervisory authorities in the EU), which was published on 11 November. The guidance is currently undergoing consultation which is due to close on 21 December, however given the level of detail set out in it, little is expected to change as a result of the consultation process.

As Dan Reavill explained at our webinar the guidance essentially sets out a two step process which must be followed when relying on SCCs as your appropriate transfer safeguard:

1. The exporter is to carry out a transfer risk assessment by analysing the destination of the exported data (ie the location of the importer), in addition to the due diligence that is required on the importer themselves, that data exporters are already accustomed to doing. This requires reviewing the destination jurisdiction's laws and practices, because the SCCs alone, which simply impose duties on the importer, are of little value if, for example, third parties are able, under the law of the destination country, to access the data without the importer's permission or knowledge. The importer is required to assist with this exercise, assessing publicly available legislation to determine, for example, whether there are effective data protection laws in place, and redress for individuals. The EDPB has also published draft guidance in this regard – the European Essential Guarantees Recommendations – which sets out the elements to be taken into account when looking at the laws of the third country. All due diligence and conclusions from the assessment must be documented thoroughly for the purpose of accountability. Where an assessment concludes that an EU standard of essential equivalence can be provided, then the exporter and importer can go ahead with the data transfer, using the SCCs as their appropriate safeguarding mechanism.

2. Where on the other hand, an assessment leads the parties to conclude that supplementary measures will be required in order to bring the level of protection of the data transferred, up to the EU standard of essential equivalence (because the laws of the third country are inadequate without such measures being taken and will impinge on the effectiveness of the SCCs as an appropriate safeguarding mechanism for data transfer), then these need to be identified and adopted. The supplementary measures are a series of technical, organisational and contractual measures as between the data exporter and importer, and the draft EDPB guidance provides a comprehensive list of examples of what these could be.

Many of the examples of technical measures are aimed at preventing access to the data overseas, for example, by using state of the art encryption, including ensuring that any decryption keys are only held by the exporter, pseudonymisation, or splitting the data between multiple processors. As has been highlighted by many organisations, data protection practitioners and IT specialists, the reality is, that many of these measures if implemented, would leave the importer unable to use the data in any meaningful way or for the objective of the transfer (for example, when transferring data to a cloud provider or other provider which is providing a service where access to the data is integral to being able to provide the service, or where you're transferring data for a shared business purpose, probably on an intra-group basis (for example, transferring a HR database)).

If technical measures alone aren't going to be sufficient, there are also contractual and organisational measures to factor in. The contractual measures are additional measures that can be built into the contract between the data exporter and importer, and they essentially build on the transparency offered by the importer to the exporter, for example, by confirming that there are no technical back doors in its IT systems that provide third party access, or offering enhanced audit rights in respect of the importer.

---

1 Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

Finally, there are organisational measures that can be taken, such as beefing up internal policies that the importer should put in place, documenting processes for data minimisation, and notification obligations where a public authority requires access to the data.

However, despite all this, the reality is that technical, contractual and organisational supplementary measures are very difficult to implement in any meaningful way, if a conclusion has been reached that the laws and practices of the destination country, do not provide a data protection standard of essential equivalence. Dan's conclusion therefore, was that organisations will find themselves in a catch 22 situation: an assessment of local laws leads them to conclude that supplementary measures are required; yet many of those measures won't be enough to provide a solution to the local law assessment. This means that in many instances exporters will be left with two choices: i) to avoid exporting personal data from the EEA; or ii) implement the supplementary measures and hope for the best.

New SCCs

The judgment in Schrems II also appears to have hastened the development of new SCCs, which had been identified as an objective when the GDPR was first implemented in 2018. The European Commission published its draft soon after the EDPB draft guidance was released. A consultation period is in place until 10 December. Once ratified, the new SCCS will have to be used for all new exports of personal data from the EEA (where standard contractual clauses are the appropriate safeguarding mechanism used by the exporter and importer). The new SCCs will also replace all existing contracts which rely on the current set of SCCs, although parties will have a sunset period of 12 months to carry out this exercise. A significant amount of re-papering is expected.

The new SCCs cover a wider set of transfer scenarios, and take a modular approach so that the relevant scenario applies to the parties signed up to them:

- Controller to controller
- Controller to processor
- Processor to processor
- Processor to controller

Whilst the modular approach of the new SCCs means that they are easier to adapt to a variety of given situations, and whilst they do attempt to address at a contractual level, some of the issues examined in Schrems II and the EDPB draft guidance, there are difficulties. Dan highlighted two in particular:

1. The provisions requiring sub-processors of data importers to have direct interaction with the ultimate data controller in certain instances (for example, breach notification where appropriate, and accepting audits by controllers as well as exporters), will be difficult to achieve in practice, particularly where sub-processors don't know the identity of the ultimate controller of the data that they process. For example, an organisation based in the EEA which sends personal data to a HR service provider located in the US, which in turn makes use of data centres located in the US. In this scenario the operator of the data centres won't necessarily know the identity of the EEA based organisation/controller.

2. Another difficulty arises from the onerous obligations that the new SCCs impose on importers to resist data access attempts by public authorities, including the requirement on the importer to exhaust all available remedies to challenge a request, which would require considerable cost to be expended on appointing lawyers, conducting litigation and so on.

The timing of the release of the draft SCCs creates particular problems for UK data processing organisations which are in the midst of preparing for the end of the transition period, following the UK's exit from the EU earlier this year.

At the end of the transition period, the UK will become a third country for the purpose of EU data protection, which means that unless an adequacy decision is granted by the EU in respect of the UK, transfers of personal data from the EEA to the UK will need to be undertaken using an appropriate safeguard, such as SCCs, or under one of the GDPR mandated derogations. Richard Ward highlighted that UK based data processors will now, in this situation, have to incorporate SCCs into their contracts with EEA based controllers. Even existing contracts will have to be revised to reflect the fact that from the end of the transition period, UK based controllers and processors will be importers of EU personal data, rather than exporters. All this will require significant re-papering, not to mention due diligence into UK legislation on public authority access to data, to reflect the requirements of Schrems II and the EDPB guidance once finalised, relatively soon after an already significant amount of papering was put in place to address the requirements of GDPR implementation some two years ago. Worse still, is if these clauses need to be updated again, once the new SCCs are adopted by the European Commission. Preparation won't just fall on UK based processors, but on EEA based controllers too.

Richard also drew attention to the broad definition of 'processing' of personal data in the GDPR, which effectively means that a number of less obvious personal data transfers will need to be taken into account as well – for example, the act of looking at personal data can, in some circumstances, constitute an international transfer. So, when looking at transfers of personal data to a data centre located in a third country for example, you would also have to consider where any support staff who might also have access to the data are located and whether that constitutes a separate data flow requiring attention.

One answer to these problems is, of course, if the EU finds that the UK provides an adequate level of data protection – in which case, provided that this comes without conditions attached, – data flows from the EEA to the UK could continue as is.

Dan concluded our look at personal data transfers out of the EEA, by summarising that the EDPB guidance together with the new SCCs would require a lot of work to be done by EEA based organisations in re-papering their current SCCs, in assessing the effectiveness of those clauses in every local jurisdiction to which data is exported, and in carrying out and implementing possibly three types of supplementary measures. Whilst common approaches will start to emerge, we haven't seen them yet, and possibly won't in time for all the work that UK based importers will have to undertake to prepare for a scenario where the EU does not grant the UK adequacy.

UK National Data Strategy

The UK Government's National Data Strategy is the latest step in a drive to make the UK a world-leader in the use and flow of data in a way which opens up opportunities for the private and public sectors in the decades ahead.

An overall National Digital Strategy is to follow so this latest document is more of a framework which continues to ask questions of its audience. But it is also revealing in indicating the areas where the Government clearly feels there are barriers to the effective use of data, both by Government and other organisations and companies.

Nicky Morgan drew a contrast between the UK where data use is seen as an opportunity rather than a threat and other regimes, including in the EU, where data protectionism seems to be on the rise. As the Strategy states, the UK wants to influence global rules on data and data use and is also clear that preserving the free flow of data is seen as essential both to drive economic growth but also for effective public service delivery. Covid-related events in 2020 have shown that where data can be shared effectively across the public sector then delivery of public services is enhanced.

Getting data use right is also seen as critical to support digital innovation, particularly in areas such as supporting UK ambitions to be a global leader in the development and use of AI and machine learning and the Internet of Things – all of these need as much data as possible to be as effective and productive as possible.

The Government has identified five 'concrete and significant' opportunities for data to transform the UK by:

- Boosting productivity and trade
- Supporting new businesses and jobs
- Increasing the speed, efficiency and scope of scientific research
- Driving better delivery of policy and public services
- Creating a fairer society for all

The Government's intentions are:

- Maximise data use domestically
- Exercise international influence on data sharing and use
- See a greater use of digital identities
- Remove barriers which limit wider use of data

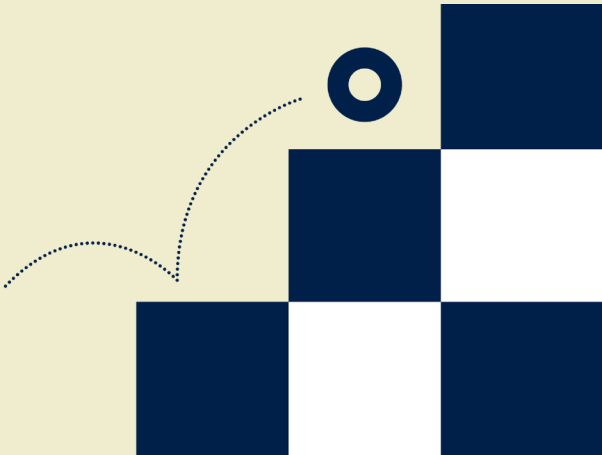
The four core pillars of the Strategy are:

- Strong data foundations
- Training people to have the right data skills
- Better data availability
- Using data responsibly

And from the pillars five missions are identified:

- Unlocking the value of data across the economy
- Securing a pro-growth and trusted data regime
- Transforming government's use of data to drive efficiency and improve public services
- Ensuring the security and resilience of our data infrastructure
- Championing the international flow of data

As Richard Ward also said at our webinar, the starting point is that people need to trust companies and organisations with their data so any changes which might be considered for the UK's future data protection regime need to bear that in mind. Richard said, "A lack of trust isn't helpful for innovation". The National Data Strategy does recognise that a balance must be found between embracing digital opportunities, whilst also keeping data subjects safe online and limiting data exploitation.



EU Data Governance Act proposals

Earlier this week the EU finally published its proposal for a Regulation on European data governance (the Data Governance Act). The sharing of both personal and non-personal data generated by public authorities, private sector organisations and individual citizens will be encouraged by introducing data governance standards which offer protection under existing EU laws such as GDPR; envisaging the setting-up of data intermediaries who will distribute data but can be trusted to do so because they are complying with strict requirements; and incorporating common European data spaces to enable data to be shared by public and private sector organisations in nine strategic domains, namely health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

Competition in digital markets

One of the most interesting debates in data law at the moment is how competition law is potentially going to be used in curbing so-called Big-Tech companies.

The UK's National Data Strategy asks whether the hoarding of data and the impact on the broader availability of data is hindering other innovators and entrepreneurs from unlocking data to generate economic growth.

This week the UK Government has announced the setting-up, from April 2021, of a Digital Markets Unit, within the Competition & Markets Authority. The CMA believes that the dominance of Big-Tech companies such as Facebook and Google and the nature of the search and online advertising markets gives them an 'unassailable incumbency advantage' that needs to be tackled with new laws. The new Unit will enforce a Code of Conduct which Big-Tech companies will sign up to with the aim of creating a level playing field for smaller businesses, giving people more control of their data and defining the relationship between online platforms and publishers including newspapers.

In recent days the CMA has also been urged to act by lobby group, Marketers for an Open Web, to stop Google unveiling a new 'privacy sandbox' as an alternative to using online 'cookies' to capture user data.

Meanwhile, at EU level there are proposals to subject large internet companies to more stringent laws designed to curb their market power. The laws are said to include forcing them to share data with rivals and be more transparent about how they gather data.

Moves are also afoot in the USA to curb the power of Google, Facebook, Amazon and Apple. In October the House of Representatives anti-trust subcommittee issued a lengthy report into anti-competitive practices by those companies. Concern about the power of Big-Tech seems to be shared across the US political spectrum, so it seems unlikely a change of White House administration in January 2021 will halt these moves.

Meanwhile the Federal Trade Commission is pursuing an anti-trust case against Facebook and the Department of Justice (supported by 11 Republican state attorneys-general) has launched a major lawsuit against Google. In the latter case Google is accused of 'supressing competition in internet search.' The US Attorney-General's comments clearly point to the concern that the perceived anti-competitive behaviour of Google will stop the next generation of innovators and even the creation of a successor to Google itself. It is unclear how this action might be resolved – are the US authorities seeking the break-up of Google or the sharing of data and access to its search capabilities?

The election of President-Elect Biden is not expected to dramatically alter these approaches in the US. As Jeannie Rhee commented at our webinar the Biden administration will not be an equivalent of a third Obama administration. They recognised that the world has changed in the intervening years, protectionism is in place and the world order is different from when senior officials last served.

With Vice-President Elect Harris who is from California due to take office it will be interesting to see if the new US administration decides to follow California's lead in approving tougher new privacy laws. While attention was focused on the US Presidential Election in early November Californians were voting on 'Proposition 24' which is expected to lead to a more comprehensive state-wide privacy law which gets closer to the EU GDPR approach.

Will it be possible to find a global consensus on data protection? As Sabina Ciofu stated, "We don't have global rules". Sabina pointed out that the WTO is making progress with a joint initiative on ecommerce and proposals on a consolidated text for next year's WTO conference. This is the only forum where US, China and the EU, plus 83 other countries, can reach agreement. In the absence of global rules, countries will also aim for bilateral and plurilateral agreements including free trade agreements that include provisions on data flows section and regulations on privacy and cybersecurity. In Sabina's view the UK-Japan trade agreement has a good ecommerce chapter, CPTPP provisions on cross border data flows, with high standards of Data Protection.

One big innovation has come from the first digital only trade agreement between New Zealand, Chile and Singapore. Other countries may join this, and it contains novel commitments on digital identity and inclusion. Singapore has also signed another agreement with Australia which goes further – includes provisions on safe online environment and digital ID.

Meanwhile the World Economic Forum has called for a Global Data Convention and we shall have to see if G20 and G7 countries both prioritise data flows and reach any agreement on protecting that data.

Key contacts

Nicky Morgan
Consultant, Technology Sector Group

nicky.morgan
@traverssmith.com
+44 (0) 20 7295 3279

Dan Reavill
Head of Commercial, IP & Technology

dan.reavill
@traverssmith.com
+44 (0) 20 7295 3260

The information contained in this booklet is based on information available at the time of publication. Travers Smith LLP has made every effort to ensure the accuracy of the information in this booklet. However, readers should always obtain profession al advice before deciding to take any action (or not, as the case may be) in relation to information contained in this booklet. Travers Smith LLP is a limited liability partnership registered in England and Wales under number OC 336962 and is regulated by the Solicitors Regulation Authority. The word "partner" is used to refer to a member of Travers Smith LLP. A list of the members of Travers Smith LLP is open to inspection at our registered office and principal place of business: 10 Snow Hill, London EC1A 2AL.