ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Online Safety Bill now law but with phased entry into force

The Online Safety Bill was agreed by Parliament on 19 September, 18 months after its first reading,[1] with Royal Assent on 26 October.[2] By **Jack Higgins** and **Rob Sumroy** of Slaughter and May.

The Online Safety Act (OSA), which imposes a host of new duties on in-scope online services will, according to the government, "make the UK the safest place in the world to be online".[3] But the Act has

Continued on p.3

From Safe Harbour to Data Bridge: Where there is trade there is a will

Alex Dittel of Wedlake Bell warns that UK businesses may still need comprehensive contracts with their US counterparts to avoid UK personal data being used for other purposes.

The UK-US Data Bridge, which entered into force on 12 October 2023 following the European Commission's earlier EU-US adequacy decision adopted on 10 July 2023, ends almost three years of uncertainty about data transfers compliant with the General

Continued on p.6

Issue 130 **NOVEMBER 2023**

UNITED KINGDOM
report

ISSUE NO 130 **NOVEMBER 2023**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Jack Higgins and Rob Sumroy
Slaughter and May

Alex Dittel
Wedlake Bell

Emma Erskine-Fox
TLT

Gabrielle Hornshaw
University of Nottingham

Merrill Dresner
PL&B Correspondent

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

MEPs raise concerns over the UK DP legislative framework

The UK's Data Protection and Digital Information (No. 2) Bill will not be over the line until some time next spring, but members of the European Parliament are already worried. Why? The EU-UK adequacy decision is in place, and now the UK has its separate arrangement with the US, mirroring that of the EU's (p.1).

The MEPs are concerned about the UK government's desire to leave the European Convention on Human Rights – the backbone of data protection frameworks. The civil liberties committee's opinion also comments on the Data Protection and Digital Information (No. 2) Bill, saying that in its current form, the Bill could further jeopardise the adequacy decision granted to the UK. The EU Commission has said it will closely monitor the situation and repeal the adequacy decisions if privacy is no longer "essentially equivalent" in the UK.

The MEPs also say the Bill would undermine the independence of the Information Commissioner's Office (ICO) and introduce powers that would allow the government to interfere with the ICO exercising its functions www.statewatch.org/media/4075/eu-ep-libe-opinion-tca-implementation-rights-10-10-23.pdf.

While helpful, the UK-US Data Bridge is not a solution to all data transfer situations due to its non-exhaustive scope. If businesses cannot use the new UK-US Data Bridge because their transfers are in sectors not covered by the framework, they will continue with Binding Corporate Rules or Standard Contractual Clauses. Other challenges remain too (p.1).

New legislation addressing online harms is now in place (p.1). The Online Safety Act will, according to the government, "make the UK the safest place in the world to be online". The government is also promoting safe AI with its international summit (p.12).

We are including an interesting management story in this issue on how Clear Channel attempts to stay clear of data protection problems in its Out of Home advertising which gathers data, but mostly non-identifiable information (p.14). Clear Channel is providing a platform for good, and uses Privacy Enhancing Technologies (PETs) to ensure that any personal data processed is necessary to provide the services. A good model for improving the bad reputation of the online advertising environment. Read more about the challenges and advantages of using PETs on p.16.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Data Bridge... from p.1

Data Protection Regulation (GDPR). The *Schrems 2* decision on 16 July 2020 elevated the "essentially equivalent" test to all levels of data transfers. It led to a flurry of compliance activity introducing transfer impact assessments (TIA) as part of supplier due diligence, and various supervisory authority findings against Google Analytics 4.0, culminating in a €1.2 billion fine against Meta for its EU-US data transfers based on standard contractual clauses (SCCs).

Going forward, UK organisations can transfer personal data to US-based commercial organisations which self-certified under the new UK-US Data Privacy Framework (DPF), without the need for a transfer mechanism (such as SCCs) or a TIA.

Many US businesses which carry on trade in the UK will likely adopt the DPF. On the other hand, not every US organisation will be ready to subject itself to the jurisdiction of the Federal Trade Commission (FTC), Department of Transport (DoT) and an independent dispute resolution mechanism, let alone the due diligence and continuous privacy programme necessary to demonstrate compliance with a regime which is no stranger to enforcement.[1]

However, SCCs (or an alternative transfer mechanism) and a TIA will still be required if the US counterparty does not abide by the DPF, either because it failed to self-certify or is within an industry excluded from DPF, such as, banking, insurance, and telecommunications companies. In those cases, the TIA should be easier to complete given the new Executive Order (EO) 14086 of 7 October 2022, concerning state surveillance. Following the adoption of the EO, the Data Bridge is a new declaration of trust in US authorities which may intercept data transferred between "economic operators" and process it for national security and public safety. Nevertheless, if the US counterparty is not a DPF participating organisation and not subject to the FTC and DoT regulatory oversight, this could slightly complicate the TIA.

Basis of the new US-EU adequacy decision

Max Schrems started his complaint following the Snowden revelations in May 2013 about the unrestricted power of US authorities to collect data for national security purposes. This was at the time of heightened state surveillance as a response to the ongoing threat of terrorism following 9/11 in 2001. Whilst the lack of safeguards against state power and remedies for foreign nationals were at the heart of the *Schrems 1* and *2* cases, these cases did not affect the sharing of law enforcement data between the US and EU.[2]

Under the authority of section 702 of the Foreign Intelligence Surveillance Amendment Act of 2008, the US National Security Agency (NSA) programme called 'PRISM' enabled the mass collection of data from companies such as Facebook. In relation to each surveillance programme, the Attorney General and Director of National Intelligence seek certification from the Foreign Intelligence Surveillance Court (FISC) ensuring that no US person is affected by the programme. The resulting FISC order which is renewed annually, is used to compel communications providers to give access to surveillance data. Enacted in 2008, FISA 702 is due to expire at the end of 2023 but will likely be renewed given the new adequacy decision.

> It is likely that DPF organisations will find ways to use UK personal data for their own purposes without meaningful limits.

The EO attempts to remedy the lack of safeguards for foreign nationals under US law. Signals intelligence activities must now take into account all persons' legitimate privacy interests. They shall be as tailored as feasible to advance a validated intelligence priority and not disproportionately impact privacy and civil liberties. They must be conducted in a proportionate manner and scope, and subjected to rigorous oversight. The EO is essential for the EU-US adequacy decision and in turn for the Data Bridge. The EO is independent from the DPF but the framework is the gateway for citizens of "qualifying sates" (which includes EU countries and the UK) to lodge "qualifying complaints" against US authorities.

A complaint by a UK individual will first be investigated by the Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence. Following that, the newly established Data Protection Review Court (DPRC) will review the CLPO's decision and issue a binding decision and direct the intelligence agencies to take remedial measures. The US Department of Commerce (DoC) will maintain a record of all complaints. Every five years, the DoC will check if information pertaining to a past complaint has been declassified, and if so, it will contact the European data protection authority with a view to informing the complainant.

UK government's approach to data transfers

The UK government has shown a strong desire to resolve the data transfer issue created by the *Schrems 2* decision. In June 2023, it announced the "first-of-its kind economic partnership" with the US setting out trade, political and defence ambitions and announcing the UK-US Data Bridge.[3] In September, the Secretary of State for Science, Innovation and Technology laid before Parliament the Data Protection (Adequacy) (United States of America) Regulations 2023 which came into force on 12 October 2023 and which designate the US as a country offering an "adequate level of protection".

In its adequacy analysis,[4] the government was satisfied that "the US respects human rights and fundamental freedoms" and the provisions of the Data Bridge and other relevant US

laws and practices provide an adequate level of protection for UK personal data, and do not undermine the level of protection that UK data subjects enjoy under the UK GDPR, when that data is transferred to DPF certified US organisations. However, one could question if a legal system without universal human rights, based on civil rights reserved for US persons, can easily be understood not to undermine the protection of personal data of UK persons who are not US citizens.

Whilst that is a question for the UK government, UK organisations must consider the limitations of the DPF.

- The DPF's distinction between a controller and an agent performing tasks (processor) is vague. Many obligations which typically rest with controllers under UK GDPR, such as notice and choice, will apply to agents. However, agents are exempt because a notice is only required "when individuals are first asked to provide personal information", which an agent would rarely do. Unlike the general transparency known under UK GDPR, the DPF notice is only triggered in specific circumstances.
- An agent must provide notice before using UK personal data for a new purpose. However, notifying a new purpose may not always be required, if providing a notice is not practicable. This will likely be the case in relation to analytics and machine learning relying on pseudonymised data.
- "Personal data" is defined as data about an identified or identifiable individual that is within the scope of the GDPR, received by an organisation in the United States from the EU. It could be argued that if the personal data is collected (rather than received) by the DPF participating organisation, it will not constitute personal data under the DPF.
- The DPF organisation could also argue that the data was anonymous when received or anonymised upon receipt. Without definitions, the DPF organisation is free to adopt any general meaning of anonymisation which could include pseudonymisation. This would also circumvent the onward transfer rules which require a contract, notice and choice.
- There are no lawful bases and no necessity assessment. Instead, DPF organisations can use personal data that is "relevant" for the purposes of processing, and personal data may be retained in identifiable form for as long as it "serves" the purpose. Arguably, any minimal relevance or utility will permit the continued processing of data.
- Choice must be provided before processing for any new materially different purpose. Without definitions, the DPF organisation can make up its own mind about what "materially different" means. Moreover, dominant US services providers could include all desirable purposes in their standard terms and then claim that all personal data was provided for those purposes.
- Change of purpose is only by choice and the choice under DPF is opt-out and not opt-in. With dark patterns encouraging people to consent, it will be even easier for DPF organisations to give individuals an obscure "opportunity to choose (i.e., opt out)" in the DPF organisation's favour. It is plausible that DPF organisations will likely find ways to recycle UK personal data for their own purposes.
- Another controller receiving UK personal data under an onward transfer must commit to respecting the individual's consent. Without definitions, this could be implied consent. Besides, if the recipient cannot comply, the controller is free to take "reasonable and appropriate steps to remediate", for example, by anonymising the data and continuing to use it.
- Unlike the UK GDPR which prescribes appropriate security measures, the DPF's security is subject to reasonableness.

The GDPR is a successful law because it has a clear objective which guides its interpretation by the courts. There is no such certainty under the Data Bridge. The FTC's mission statement to protect the public suggests that it will err on the side of higher individual protections. However, the UK government notes that "some vagueness" remains. Given the lack of definitions and interpretation rules, there is plenty of scope for "creative" interpretation. Some could argue this undermines the protections afforded under the UK GDPR.

UK controllers and processors must be alert to these shortcomings. Without a comprehensive contract that introduces more clarity beyond the usual Article 28 data processing terms, it is likely that DPF organisations will find ways to use UK personal data for their own purposes without meaningful limits. Simply agreeing that the US organisation will comply with DPF will not be enough to protect the UK organisation's personal data.

The ICO's concerns

Following the *Schrems 2* decision, the ICO criticised the binary approach of adequacy agreements which excludes many countries.[5] By introducing the "sufficiently similar" instead of the "essentially equivalent" test, it paved the way for more inclusive TIAs. It did not engage in any noticeable enforcement of the decision and data transfers from the UK have not suffered.

In its merely advisory role in the adequacy process, the ICO agreed that "it is reasonable for the Secretary of State to conclude that the UK Extension provides an adequate level of data protection". However, the ICO mentioned "there are four specific areas that could pose some risks to UK data subjects (author's note - perhaps tactically not saying "undermine protection") if the protections identified are not properly applied".

- Lack of a definition of "sensitive information" under DPF could mean that "protections may not be applied in practice".
- Lack of equivalent protections in relation to spent convictions and the ICO is "not clear how these protections would apply".
- Lack of a substantially similar protection from decisions based solely on automated processing and the right to obtain a review of an automated decision by a human.
- Lack of substantially similar right to be forgotten nor an unconditional right to withdraw consent.

Instead of owning up to the tasks, the ICO has recommended that the Secretary of State should monitor these areas closely. Moreover, the ICO endorses the proposal for the government to prepare

guidance for UK organisations in adopting better definitions in their contracts with DPF organisations. However, many UK organisations will not have the negotiating power to impose terms with US organisations. Perhaps, what is needed are mandatory model clauses instead, but this has not been proposed.

Conclusion

Whilst the Data Bridge will enable an SCC-free and TIA-free flow of personal data for trade between UK and US organisations, it is clear that the DPF poses various risks. Without comprehensive contracts with their US counterparts, UK organisations could find that their personal data is used beyond what was envisaged. However, without mandatory model clauses issued by the government, few UK organisations will be able to dictate terms to large US organisations.

The Data Bridge could be criticised for lowering the protection under UK GDPR. On the other hand, the strict *Schrems 2* rules could perpetuate discrimination against countries, and the rules remain too complex for most organisations to apply. Perhaps a more inclusive solution is needed, as data transfers have become an international phenomenon with many new frameworks emerging. In this regard, the DPF certainly sets an acceptable standard.

We will not have to wait for privacy advocates to keep this conversation alive. In a recent case T-553/23 R,[6] the Court of Justice of the European Union rejected an application for interim measures to suspend the EU-US adequacy decision on the basis of serious and irreparable harm, lack of due diligence on DPF organisations, lack of adequate level of protection provided under US law, a lack of compliance with human rights, and a lack of proper review. A challenge to the EU-US deal would likely also affect the Data Bridge and the UK's ambition to retain its adequacy status.

AUTHOR

Alexander Dittel is a Technology Partner at Wedlake Bell.
Email: adittel@wedlakebell.com

REFERENCES

1 Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield (https://www.ftc.gov/news-events/news/press-releases/2019/09/five-companies-settle-ftc-allegations-they-falsely-claimed-participation-eu-us-privacy-shield).
2 US-EU Data Protection and Privacy Agreement entered into in December 2016, and extended on 21 July 2022 to the UK following Brexit.
3 UK and US launch first-of-its kind economic partnership, 8 June 2023 (www.gov.uk/government/news/uk-and-us-launch-first-of-its-kind-economic-partnership).
4 Analysis of the UK Extension to the EU-US Data Privacy Framework, Department for Science, Innovation & Technology, September 2023 (assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1185427/analysis_of_the_uk_extension_to_the_eu-us_data_privacy_framework.pdf).
5 A Bretton Woods for data, 9 September 2021 (ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/09/a-bretton-woods-for-data/).
6 *Philippe Latombe v European Commission* (Case T-553/23 R) (curia.europa.eu/juris/document/document.jsf?text=&docid=278542&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=225583)

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"The *PL&B UK Report* is an extremely useful tool for our office, keeping us in touch with global data protection issues and developments as they happen. As a 'third country', this is vitally important in ensuring the JOIC remains both current and relevant, particularly in this post-GDPR world."

Paul Vane, Information Commissioner, Jersey Office of the Information Commissioner

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.