Tools for Schools Limited: Data Transfer Impact Assessment – US (Google Cloud)

Contents

Introduction

Tools for Schools Limited (**TfS**) uses Google Cloud to host the data that is required to run the Book Creator application provided by TfS. Currently, TfS uses Google Cloud servers in the USA and relies on UK- and EU-approved standard contractual clauses (**SCCs**). As such, in accordance with the *Schrems II* judgment of the Court of Justice of the European Union (**CJEU**) on 16 July 2020, TfS is required to conduct an assessment of US data protection laws and establish whether supplementary measures are required to be put in place in order to ensure that relevant laws do not impinge on the protections provided by the SCCs. At the time of completion of this data transfer impact assessment (**DTIA**), new EU-approved SCCs have been finalised and a transition period of 18 months to move to the new SCCs has commenced. A draft set of UK clauses (template international data transfer agreement or **IDTA**) has been issued, alongside a draft UK addendum to the EU-approved SCCs. As such, Google has not yet transitioned to the new EU-approved SCCs or the UK IDTA/addendum. This transition will take place before the end of the required transition period.

Section 1 is the “fact gathering” section which sets out details of data protection laws, rules, procedures and practices in the US. This is purely a factual assessment that does not detail the risks of the particular transfers.

Section 2 is the data transfer impact assessment itself, which looks at the risks of the particular transfers and other factors, including additional safeguards and supplementary measures available, in order to provide an assessment of the overall residual risk of the particular transfers.

Section 1: Fact gathering

This section sets out details of the US's data protection framework and the laws applicable. It addresses all of the key principles of the General Data Protection Regulation (**GDPR**) and assesses the level of protection provided by US laws in respect of each of those principles.

This section has been completed by UK counsel from a UK perspective, based on input from US lawyers, but does not constitute US legal advice.

The "Response" column includes details about the applicable laws and rules.

The "Risk" column sets out:

- the risk level of US laws in relation to each specific question, without taking into account any mitigating measures or considerations (this will be taken into account in Section 2); and

- the overall risk for each principle where indicated, factoring in the risk level attributed to each question relating to that principle.

Question	Response	Risk
Part 1: Basic Concepts	**Overall risk for principle:**	**L**
Are contractual safeguards provided by the SCCs likely to be enforceable in the Third Country?	Yes. There is an established and respected federal and state legal system in the US, demonstrating that the US respects the rule of law. There are no indications that contractual obligations will not be enforceable and although the US is not a party to any conventions/multi-lateral agreements for recognition or enforcement of foreign judgments, there are a number of federal and local laws that mean that the US courts generally recognise and enforce most final foreign judgments (subject to certain conditions). The US is a party to the UN Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention) and the	L

	Inter-American Convention on International Commercial Arbitration (the Panama Convention)[1] and therefore will typically enforce foreign arbitration award. Third party beneficiary rights under contracts are recognised and enforceable.	
What laws and/or rules are in place (**data protection rules**) governing the collection and use of personal data?	The US data protection framework comprises a layered web of national privacy laws and regulations that are sector- or issue-specific, together with state privacy and data security laws, and federal and state prohibitions against unfair or deceptive business practices, including actions that are contrary to representations made by commercial enterprises in their published privacy policies. The US Federal Trade Commission (FTC) is the primary government agency at the federal level with jurisdiction and enforcement powers over the privacy practices of most commercial entities, pursuant to the Federal Trade Commission Act (FTC Act)[2]. The FTC has the authority to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices. The FTC uses its authority in relation to data protection to issue regulations in certain areas, enforce certain privacy laws and take enforcement actions and investigate companies for: ■ failing to implement reasonable data security measures; ■ making materially inaccurate privacy and security representations, including in privacy policies; ■ failing to abide by applicable industry self-regulatory principles;	L

[1] https://www.gibsondunn.com/wp-content/uploads/documents/publications/Edelman-Jura-Enforcement-of-Foreign-Judgments-US.pdf
[2] https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

- violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of the FTC's consumer privacy framework or certain national privacy laws and regulations.

There is also federal legislation that imposes privacy and data security requirements on various industry sectors (e.g., regulations applicable to financial institutions, personal health information, credit report information and direct marketing) as well as specific issues (e.g. the protection of children's personal information). Also important in the overall US data protection scheme is the Federal Privacy Act of 1974[3], as amended, 5 U.S.C. § 552a, which establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Although this law applies to federal agencies only, these requirements generally are flowed down to government contractors and therefore have had broader impact on commercial practices in the US.

The Financial Services Modernization Act 1999, more commonly known as the Gramm-Leach-Bliley Act (GLBA)[4] is the principal framework for collection, use, and disclosure of financial information. The GLBA prohibits disclosure of non-public personal information, that is, any information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. Companies subject to the GLBA are also required to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared with third parties. Other federal rules on the protection of financial data include the Disposal Rule[5] and the Red Flags Rule[6]. At the state level, Attorneys General have enforcement powers similar to those of the FTC in relation to unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. There are hundreds of privacy and data security laws in place at the state level across the US that impose various requirements for

[3] https://www.justice.gov/opcl/privacy-act-1974

[4] https://www.congress.gov/bill/106th-congress/senate-bill/00900

[5] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/disposal-consumer-report-information

[6] https://www.finra.org/rules-guidance/key-topics/customer-information-protection/ftc-red-flags-rule

	safeguarding data, disposing of data, publishing privacy policies and notifying data breaches involving certain types of personally identifiable information. By way of example, the California Attorney General has the authority to enforce the California Consumer Privacy Act 2018 (CCPA)[7] and 25 other state privacy and data security laws. The CCPA applies horizontally and adopts many of the definitions, data subject rights and requirements of the EU General Data Protection Regulation.	
Are there any additional rules or laws that are pending implementation?	Several different consumer privacy bills have been introduced in the US Congress. In light of calls by many industry and consumer groups, the Biden Administration may progress one or more of these bills going forwards. Similarly, a number of bills are under consideration by legislatures in several states across the country, which have been side-tracked by the COVID-19 pandemic but are now beginning to gather steam once again (e.g. Washington State). Most notably, in June 2021, US Senator Kirsten Gillibrand announced the reintroduction of the Senate Bill 2134 for the Data Protection Act of 2021. This would establish a federal "Data Protection Agency" to oversee data protection practices and protect privacy rights, including by introducing an ability for the Agency to create and enforce federal data protection rules[8]. The Bill will need to pass the Senate and the House before becoming law but it demonstrates a move towards more streamlined federal privacy protections in the US.	L
Has the country previously applied for a European Commission and/or UK adequacy decision and been unsuccessful?	Yes, the European Commission has issued two separate decisions making adequacy findings in regard to the US-EU Safe Harbour and the US-EU Privacy Shield frameworks that were agreed between the US Government and the EU and approved by decision of the European Commission[9]. Both decisions of the Commission have been invalidated by the Court of Justice of the EU[10]. Both the European Commission and the US Government have issued statements indicating that they will work together to adopt a new framework that will meet the adequacy criteria of the GDPR. Post-Brexit, the UK has the power to make its own adequacy decisions. The US has not yet applied for a UK adequacy decision. It is likely that the UK and the US will also be in ongoing discussions as to a potential adequacy finding.	H

[7] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

[8] https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data

[9] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520 and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[10] https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf and https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

To whom do the data protection rules apply? Are there any exemptions/specific requirements for particular types of organisations, such as public authorities or law enforcement/national security/defence agencies?	As indicated above, the FTC has broad powers to take action against most commercial entities (with the exception of sectors that are regulated by other government authorities) that violate the terms of their privacy policies. Individual state and federal laws relevant to particular sectors or issues apply within the scope of their respective jurisdictions. In general, consumer data protection laws do not apply to federal or state government agencies, but there are constitutional protections at both federal and state levels relating specifically to citizens' privacy, due process and fundamental rights against search and seizure (which has been broadly defined by the courts to cover privacy rights in various contexts).	L
Who is protected by the data protection rules? Are any persons (e.g. children or vulnerable people) treated differently, and if so, how?	Because the US framework tends to focus on the protection of consumers in certain sectors (e.g., financial services, health care, credit vetting) and vulnerable individuals (e.g., children), the question of who is protected by the various laws (as described above) will generally depend on the scope of the federal or state privacy/data security law in question. As noted above, the FTC Act and state equivalents, as well as the CCPA, apply horizontally and apply broadly to all types of consumers and types of personal information, with the exception of individuals who are under the protection of sector-specific legislation, which takes precedence.	L
What types of data do the data protection rules cover? Are any types of personal data treated differently, and if so, how?	As noted above, the US framework tends to focus on the protection of consumers in certain sectors (e.g., financial services, health care, credit vetting) and vulnerable individuals (e.g., children). Therefore, the question of what types of personal data are protected will generally depend on the scope of the federal or state data. In the financial services sector, as noted above, the GLBA prohibits disclosure of non-public personal information, which is more broadly defined than personally identifiable information. Regulations issued under this statute define "personally identifiable financial information" as: ■ any information an individual provides to obtain a financial product or service; ■ any information about an individual from a transaction involving a financial product or service; or	L

	■ any information about an individual in connection with providing a financial product or service.	
What types of processing do the data protection rules cover? Are any types of processing treated differently, and if so, how?	As noted above, the US framework tends to focus on the protection of consumers in certain sectors (e.g., financial services, health care, credit vetting) and vulnerable individuals (e.g., children). Therefore, the question of what types of processing are protected will generally depend on the scope of the federal or state data privacy/security law in question. The FTC Act and state equivalents, as well as the CCPA, apply horizontally and apply broadly to all types of processing of personal information in scope. In California, the "sale" (as broadly defined, and essentially meaning "disclosure for consideration") of personal information is subject to specific requirements and data subject rights, as is the collection and processing of personal information for other purposes.	L
Part 2: Transparent, lawful and fair processing	**Overall risk for principle:**	**M**
Do the data protection rules require particular lawful grounds or justifications to be in place to process personal data? Are there any exemptions or specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	The horizontal data privacy laws in the US focus primarily on ensuring that there is adequate and accurate notice and transparency in relation to the processing of personal data. (Sector-specific legislation often requires the consumer's prior consent to processing.) In most cases, government authorities may only obtain access to non-public data about individuals if they obtain a warrant from the appropriate judicial authority following due process by, among other things, demonstrating that there is probable cause to believe that the individual in question may have committed a crime which constitutes a national security risk as defined under the relevant statutes. There are two main exceptions to the requirement that traditional warrants be obtained showing probable cause as to the particular individuals whose data is sought. Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)[11], a warrant may be obtained to require providers of "electronic communications services" (e.g., telecommunications operators and "remote computing" companies like Facebook) to facilitate the bulk collection of personal data about multiple individuals without a showing of probable cause. There is also an Executive Order issued by the Obama Administration (EO	M

[11] https://icontherecord.tumblr.com/topics/section-702

	12333)[12] which, under specified circumstances, authorises the collection of data stored outside the US pertaining primarily to non-US citizens for national security purposes. For more information, see part 10 below.	
Do the data protection rules impose obligations on organisations to inform individuals how their data will be processed? Are there any exemptions or specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	As noted above, the US framework tends to focus on the protection of consumers in certain sectors (e.g., financial services, health care, credit vetting) and vulnerable individuals (e.g., children). Therefore, the question of what type of notice of data processing must be provided will generally depend on the scope of the federal or state data privacy/security law in question. The FTC Act and state equivalents, as well as the CCPA, apply horizontally and impose rather strict requirements that are in line with the fair processing principles embedded in the GDPR. Indeed, the CCPA's notice requirements are as detailed as those contained in the GDPR, if not more so. For example, a principle tenet of the CCPA is to properly inform individuals regarding the types of personal data being processed, for what types of activities, for what types of purposes, and by what types of entities. Similarly, in the financial sector the GLBA requires companies to provide notice of their privacy practices and in the health care sector, very specific notices are required when personal data that is subject to the Health Insurance Portability and Accountability Act (HIPAA)[13] is collected. In line with the FTC Act, when a commercial entity that offers a good or service provides a privacy notice, the FTC and State Attorneys General can and do pursue enforcement actions against them if their statements are unfair or deceptive. This includes changes in the practices covered by such privacy notices. (C2) In the case of FISA Section 702 warrants issued to providers of electronic communications services or foreign data collection by national security agencies pursuant to EO 12333, there is no requirement that the government agencies involved notify affected individuals that their data is being collected. In the case of FISA Section 702 warrants, the recipient of the warrant is prohibited from notifying the affected individuals, and EO 12333 collections by their nature are carried out surreptitiously by national security agencies outside of the US.	M
Part 3: Purpose limitation	**Overall risk for principle:**	**L**
Do the data protection rules place any restrictions on using personal data for purposes other than those for which the personal data was originally	Most US data protection laws require that personal data be used either for the specific purpose it was collected, or for the purpose for which it was collected and any purposes that are reasonably related to that purpose. Governmental access to	L

[12] https://www.archives.gov/federal-register/codification/executive-order/12333.html

[13] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

collected? Are there any exemptions or specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	personal data would typically be limited to the purposes for which it was collected in that instance, such as by warrant in regard to a particular investigation. Even where personal data is collected pursuant to a FISA Section 702 warrant, it may only be used for the particular purpose(s) approved by the FISA Court. For more information, see part 10 below.	
Part 4: Data quality and proportionality	**Overall risk for principle:**	**M**
What obligations do the data protection rules impose on organisations to ensure personal data is kept accurate and up-to-date?	Most data protection laws in the US do not specifically require that personal data be kept accurate and up-to-date. Some laws do require the ability for individuals to challenge inaccurate information and otherwise request updates, such as laws related to credit reporting agencies and the need for their reporting to accurately reflect an individual's credit status.	M
Do the data protection rules contain controls in relation to how much personal data can be processed?	The concept of data minimisation is not incorporated in all US data protection laws, but it is implicit in the provisions of some. For example, the CCPA requires that the use of personal data must be "reasonably necessary and proportionate to achieve the operational purpose" for which it was collected.	M
Part 5: Data retention	**Overall risk for principle:**	**M**
Do the data protection rules contain controls in relation to how long personal data can be stored and/or processed for?	US data protection laws do not always contain restrictions on retention. There are examples of laws that contain specific retention provisions. The CCPA contains the role of a "service provider" that is roughly equivalent to a "processor" under the GDPR, and similarly service providers must return or delete the personal data at the end of the processing. The New York State Department for Financial Services regulations[14] require relevant entities to have appropriate record retention policies and procedures. A further example is the Illinois Biometric Information Privacy Act[15] which requires that an entity that collects biometric identifiers permanently destroy this data either within three years of the law interaction an individual has with the entity, or when the purpose for collecting the data has been satisfied, whichever comes first. Retention of materials like medical records is managed through state laws.	M
Part 6: Security and confidentiality	**Overall risk for principle:**	**L**

[14] https://www.dfs.ny.gov/industry_guidance/regulations

[15] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Do the data protection rules impose security requirements to protect against risk such as accidental disclosure of personal data?	Data security is an overarching concern of most US data protection laws. For example, the CCPA requires there be reasonable security in place to protect personal data. The Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth[16] requires a comprehensive and written information security program for entities that handle personal information of its residents. Likewise, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)[17] requires those subject to the Act to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information. The California Internet of Things Security Law[18] requires reasonable security features be built into the devices, and for certain specific security procedures to be implemented, such as default passwords that are unique to the device. There are also sector-specific laws regarding the protection of personal data in medical and financial records, and other sensitive personal data. For example, the Safeguards Rule (implemented under the GLBA)[19] requires financial organisations to develop, implement and maintain a comprehensive information security programme. This involves identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and assessing the sufficiency of any safeguards in place to control these risks.	
What processes must take place in the event of a security breach or other breach of data protection rules?	All 50 states and the US territories have enacted data breach notification laws that aim to protect "personally identifiable information," which is defined in various ways across the US. Most focus on access or exfiltration of PII by unauthorised third parties that could give rise to identity theft or other harm to consumers. Different states have different triggers for when notifications to State Attorneys General and to the affected consumers are required, and establish the time frames for and content of the notifications. Attorneys General can and do investigate data breaches following notification (or in the event of failure to notify within the statutory deadlines or otherwise comply with the applicable requirements). Similar breach notification requirements are imposed at the federal level for specific sectors (financial services, health care etc.). In December 2020, banking regulators jointly announced a proposed rule that would require banks to notify regulators within	L

[16] https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the

[17] https://www.nysenate.gov/legislation/bills/2019/S5575

[18] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[19] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

	36 hours of a “computer-security incident” that rises to the level of a “notification incident.”[20] The proposed rule would also affect companies that provide certain services to those banks, including data processing.	
Part 7: Data subject rights	**Overall risk for principle:**	**L**
Do the data protection rules provide individuals with any rights over their personal data? If so, what are these rights? Are there any limitations on these rights?	Various US data protection laws provide for rights for individuals. For example, the CCPA establishes consumers’ right to know (access), a right to delete, a right to opt-out of the sale of personal data, and a right to not be discriminated against for exercising the other rights. HIPAA also provides individuals whose personal information is processed subject to the law a right to access the personal data that is held about them. The Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)[21] provides individuals with the right to object to receiving commercial marketing communications.	L
Part 8: Onward transfers	**Overall risk for principle:**	**M**
Do the data protection rules place restrictions and obligations on onward transfers of personal data outside the Third Country?	In general, international transfer restrictions relating to personal data do not apply in the US by operation of law.	M
Can personal data be transferred freely (i.e. without any further safeguards) to any specified countries, territories or sectors or international organisations? If so, on what grounds are these countries chosen and how does the assessment process work?	There are minimal restrictions on transfers to foreign countries. These are primarily tied to personal data that is processed in relation to certain work with the US government. However, it is common practice for entities in the US to bind themselves contractually (as well as downstream vendors) not to engage in onward transfers or to adopt other contractual safeguards and protections in regard to such transfers.	L
When data is not permitted to be transferred freely, what additional safeguards are specified for transfers to other countries, sectors etc.?	See response to the first question in this section.	M
Part 9: Direct marketing	**Overall risk for principle:**	**L**
Do the data protection rules impose specific requirements on organisations when processing personal data for direct marketing purposes?	There are several different federal laws that apply to marketing. The Telephone Consumer Protection Act (TCPA)[22] regulates calls and text messages that are made to mobile or residential phones for marketing purposes or when using automated dialling	L

[20] https://www.federalregister.gov/documents/2021/01/12/2020-28498/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank

[21] https://www.ftc.gov/enforcement/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act

[22] https://www.fdic.gov/regulations/compliance/manual/8/VIII-5.1.pdf

	systems or pre-recorded message content. CAN-SPAM requires that all entities making commercial marketing provide an option to easily opt-out of the marketing messages.	
Part 10: Surveillance/access by public authorities	**Overall risk for principle:**	**H**
Are there any provisions in the data protection rules or other domestic laws which subject organisations in the Third Country to provide public bodies, law enforcement agencies or national security agencies with access to personal data held by those organisations for national security, surveillance or criminal law enforcement purposes?	Organisations can be required by law enforcement and national security authorities to provide personal data pursuant to traditional warrants issued by courts subject to due process (e.g., requiring a showing of probable cause) . Companies that are subject to such warrants may challenge them in court on the basis that they are not legally justified. For a discussion of FISA Section 702 warrants, which are an exception to this rule, please see relevant responses provided in Parts 2 and 3 above. The Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, broadly prohibits the interception and disclosure of wire, oral and electronic communications, as well as the manufacture, distribution and possession of such interception devices. At the same time, it establishes a detailed regulatory regime under which federal and state government authorities may, in certain criminal investigations, intercept, disclose and use such communications as evidence. Originally the Wiretap Act only applied to 'oral' and 'wire' communications but the Electronic Communications Privacy Act of 1986 broadened the application of the statute by expanding the kinds of communications to which the statute applied to also cover 'electronic' communications. Whereas the Wiretap Act applies to the live interception of communications, the Stored Communications Act (SCA)[23] applies to the collection of stored communications maintained by third-party service providers. The SCA generally prohibits the unauthorised access of a facility through which an electronic communication service is provided. In an effort to assist organisations in assessing whether their transfers offer appropriate data protection in accordance with the CJEU's ruling in Schrems II[24], the US government prepared a White Paper in September 2020[25] which outlines the "robust limits and safeguards" in the US pertaining to government access to data. In particular, the White Paper focuses on the concerns that the CJEU had in relation to FISA Section 702 and EO 12333.	H

[23] https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

[24] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

[25] https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

	In relation to FISA Section 702, the White Paper concludes that the Foreign Intelligence Surveillance Court (FISC) is actively involved in supervising whether individuals are properly targeted. The government must record in every case the reason a specific person was targeted and targeting procedures are approved annually by the FISC. The White Paper also outlines three separate means of individual redress for violations of FISA Section 702, under section 1810 of FISA, section 2712 of the Electronic Communications Privacy Act and section 702 of the Administrative Procedure Act. It also notes that numerous additional privacy safeguards have been added to FISA Section 702 since 2017. In relation to EO 12333, the White Paper states there is no "requirement" for a company to disclose any data to the US government and the government may not legally require US companies to disclose the data transferred under SCCs "in bulk".	
What are the general human rights regulatory standards in comparison to the UK's and the European Union's?	Good. Various data scores comparing how governments protect and respect human rights indicate that the US does not score as highly as the UK.[26] Although the United States Constitution and Bill of Rights provide broad civil rights protections, there has been criticism from human rights groups on the practices and policies of the Trump Administration, particularly in relation to the disengagement from international human rights standards.[27] However, the Biden Administration announced in February 2021 that it will reengage with the United Nations Human Rights Council, three years after forfeiting its membership[28].	L
Do the data protection rules include adherence with any international data instruments or data protection safeguards?	Yes. The US has entered into Mutual Legal Assistance Treaties with a number of countries including the UK and every member of the EU for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws. It is also a member of the Budapest Convention on Cybercrime[29] which serves as a framework for international cooperation between parties to the Convention regarding the exchange of evidence and information in cybercrime-related matters, including electronic data. The US entered into a CLOUD Act Agreement with the UK in 2019[30] which makes it easier	M

[26] See for example, https://ourworldindata.org/human-rights, as at 2017 the US scores at 0.24 while the UK scores at 2.22

[27] https://ourworldindata.org/human-rights

[28] https://www.nbcnews.com/politics/joe-biden/biden-administration-rejoin-u-n-human-rights-council-another-reversal-n1256997

[29] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[30] https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists

	for US and British law enforcement agencies, with appropriate authorisation, to obtain electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from communication providers / technology companies based in the other country.	
Do the above laws or the data protection rules contain clear, precise and accessible rules on the access and use of personal data for national security, surveillance or criminal law enforcement purposes?	The Wiretap Act requires law enforcement authorities to obtain a judicial order authorising interception of affected communications, based on a showing of probable cause that particular communications evidencing one of the crimes covered by the statute (consisting of serious felonies) will be obtained through the intercept. The SCA details requirements that law enforcement authorities must meet in order to require a third-party service electronic communications or remote computing service provider to disclose stored electronic communications. In this regard, the SCA generally requires law enforcement authorities to obtain a search warrant in order to compel such a provider to disclose the contents of stored electronic communications. In respect of Section 702 FISA, see part 10(a) and parts 2 and 3 above.	M
Do the data protection rules include the obligation for public bodies, law enforcement agencies or national security agencies to perform a necessity and proportionality test before processing personal data?	To a certain extent, yes. As noted above, the various federal and state laws that regulate the use of personal data for national security, surveillance or criminal law enforcement purposes contain various safeguards reqarding necessity and proportionality. For example, an application under the Wiretap Act must show that the surveillance will be conducted with procedures in place to minimise the interception of communications irrelevant to the investigation. In the case of a FISA Section 702 warrant, there are strict targeting procedures to specify how a “selector” (that is, an account identifier such as an email address) may be “tasked” to acquire foreign intelligence.	M
Do the data protection rules guarantee that personal data of individuals will be protected against the risk of abuse by public bodies, law enforcement agencies or national security agencies?	Yes. As noted above, there are various safeguards within the various federal and state laws to protect against the risk of abuse by national security enforcement bodies, including PPD-28.	M
Is there an independent oversight mechanism to review the lawfulness of access to individuals’ personal data by public bodies, law enforcement agencies or national security agencies?	The courts are the primary mechanism for oversight of privacy protections, particularly in the criminal context. As noted above, for searches or surveillance of electronic communications, generally a warrant or judicial order is required from the appropriate judicial authority following due process. Moreover, in the event that evidence gathered through such searches or surveillance is used as criminal evidence against a person,	M

	the person may challenge the admissibility of the evidence (including challenging the validity of the warrant or judicial order) if it was obtained in an unconstitutional or otherwise unlawful manner. US laws also provide electronic communication service and remote computing service providers with a mechanism to challenge orders compelling disclosure of customer communications. Both the SCA and FISA contain such provisions. In addition, the USA FREEDOM Act[31] brought more transparency to government surveillance activities, including by requiring the reporting of certain information to Congress and the public each year and requiring FISC to make their orders publicly available if they are deemed to address any novel Fourth Amendment legal interpretations. Additionally, this Act allows companies to issue more detailed data about the demands for user information that they receive from the government. For instance, a number of organisations now release an annual transparency report indicating a range of national security letters ('NSLs') and other information requests they have received from the government.	
Do organisations in the Third Country have any rights to reject access requests by public bodies, law enforcement agencies or national security agencies to personal data and, if so, on what grounds?	Any organisation served with a warrant, subpoena or other form of legal process requiring disclosure of personal data it has received may seek to challenge the legitimacy of the order and seek to quash it in court if it believes the order is somehow unlawful. In particular, an organisation may challenge such process on the ground that it would require them to violate foreign data privacy laws. In the face of such a challenge, if the court finds there to be a true conflict of laws, the court will apply a balancing test that weighs the US interests in enforcing the process against the interests of the foreign sovereign.	M
Part 11: Accountability	**Overall risk for principle:**	**L**
Are there requirements under the data protection rules to build privacy by design into products/solutions?	US data protection laws generally do not require privacy-by-design.	M
Are there mandatory requirements to carry out data protection impact assessments or other types of	Sector-specific laws that apply in highly regulated sectors often include assessments to be made that are similar to DPIAs. For example, the New York Department of Financial Services has cybersecurity regulations[32] for entities that operate within the financial services industry. These regulations require these entities to perform a risk assessment	L

[31] https://www.congress.gov/bill/114th-congress/house-bill/2048/text

[32] https://www.dfs.ny.gov/industry_guidance/cybersecurity

risk assessment when carrying out high risk processing?	and implement an appropriate security programme that is designed to detect and respond to cyber attacks to which the entity may be exposed. HIPAA has a specific requirement to conduct a security analysis regarding risks to electronic personal health information.[33]	
Part 12: Regulation and enforcement	**Overall risk for principle:**	**L**
Do the data protection rules specify penalties or sanctions for failure to protection personal data/failure to comply with the requirements of the data protection rules?	The penalties for violations of data protection laws vary considerably. CCPA allows for a personal right of action in the event an individual's sensitive personal data is breached, with penalties of $100-750, or actual damages, whichever is higher. It also allows the California Attorney General to fine entities that are not in compliance with the CCPA $2500 for non-compliance, and $7500 for wilful non-compliance, per violation. The FTC has limited laws under which it can immediately fine entities, and instead it will issue a consent decree that usually has a period of 20 years and requires things such as bi-annual audits, reportings on data protection activities and inclusion of board-level supervision of data protection compliance. If these orders are violated the FTC can then sue to enforce the order and obtain monetary penalties. These penalties have reached into the tens of millions of dollars. Other laws, such as the Child Online Privacy Protection Act (COPPA)[34] allow for immediate fines for violations, which range from $14,000 for negligent violations to $42,000 for wilful violations, per violation. Some data protection laws do not provide for enumerated fines, but apply the standard enforcement authority that the State Attorney General otherwise has.	L
Which body or bodies regulate and enforce the data protection rules? To what extent are those bodies independent from the government?	As discussed in greater detail in Part 1, the primary bodies that enforce data protection laws are the FTC and State Attorneys General. However, there are a variety of other sector-specific regulators that also have jurisdiction over specific data protection laws. There are also industry entities that may enforce industry codes, such as the Payment Card Industry's ability to enforce its Data Security Standard[35]. The FTC is an independent regulatory authority insofar as its Commissioners are appointed by the President and confirmed by the Senate, are required to be from different political parties, are subject to term limits and cannot be removed except for cause.	L

[33] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[34] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[35] https://www.pcisecuritystandards.org/about_us/

What powers and responsibilities do regulators have to enforce data protection legislation? What resources do they have and how are they funded?	US data protection laws are primarily enforced by regulators, as discussed above. They have broad authority and are generally funded by federal and state budget allotments that dictate their available resources. However, the California Attorney General obtains additional funding from penalties that are imposed on entities found to have violated CCPA.	L
Do regulators issue specific guidelines or recommendations in relation to data processing/compliance with the data protection rules?	Yes, the FTC and State Attorneys General will issue guidance and regulations as appropriate. Other regulatory entities will issue guidance and regulations when within the scope of their rulemaking and guidance authority, typically in relation to sector-specific laws for which they are the primary enforcing regulator.	L
What evidence is there that breaches of data protection rules are appropriately enforced?	Regulatory enforcement of data protection laws has been a feature of the US framework for many years and activity in this area has increased in recent years. There are regular orders and settlements that are announced at the state and federal levels, with the FTC taking the leading role at the federal level. Attention to data protection laws and requirements has continued to increase in recent years as regulators have grown ever more active in their enforcement. In its Privacy and Data Security Report for 2019[36], the FTC stated that it had brought enforcement actions addressing a wide range of privacy issues in a variety of industries, including social media, ad tech, and the mobile app ecosystem. These matters included more than 130 spam and spyware cases and 80 general privacy lawsuits. Details of more recent enforcement action are also available on the FTC's website[37].	L
Part 13: Redress for data subjects	**Overall risk for principle:**	**H**
How can individuals seek redress for infringement of their data protection rights or breach of the data protection rules? Are there any limitations on these rights, in particular for individuals who are not citizens of the Third Country?	Individuals can bring a complaint to a regulator that a company is not complying with data protection laws. There is also strong activity in bringing stand-alone or class-action lawsuits against entities that suffered breaches of sensitive personal information, or in other instances where individuals are afforded the right to bring a personal claim against a company for such a violation. In order to bring a lawsuit, the individual would need to demonstrate it meets the applicable jurisdiction standards to bring the claim as requested. The US Constitution does not apply to non-US citizens outside the US and therefore the protections in the Fourth Amendment do not apply to non-US citizens abroad. As	H

[36] https://www.ftc.gov/reports/privacy-data-security-update-2019

[37] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement

	noted above, FISA, which specifically permits foreign intelligence surveillance of non-US persons located outside the US, provides for multiple layers of oversight from the executive branch, the FISC and congressional intelligence committees. Additionally, through PPD-28, the executive branch has extended some limitations designed to ensure that even signals intelligence activity directed towards non-US citizens abroad is as tailored as feasible, taking into account the availability of other sources of information.	
What evidence is there that individuals are able effectively to get redress for breaches or infringements of their rights, either with regulators, the courts or other administrative bodies?	There is a considerable amount of activity related to data protection in many states and at the federal level. In instances where there are violations of the law that impact personal data, the regulators regularly investigate and issue penalties. There are also regular successes in court cases brought for breaches of personal data. These often result in class action settlements, the proceeds of which are divided between the applicable members of the class that brought the action	M
Part 14: Additional information	**Overall risk for principle:**	**L**
Do the data protection rules apply differently to any foreign nationals, citizens or residents, if not covered above?	This will depend on the subject matter and jurisdictional scope of the relevant laws. Details are set out above in respect of each relevant principle.	L
Are there any exemptions to data protection rules that are not covered above?	Not that we are aware of.	L
Are there any other concerns about the effectiveness of enforcement that are not covered above?	Not that we are aware of.	L

Section 2: Data transfer impact assessment

This section assesses the risks identified above in the context of the specific transfers and safeguards available and considers the level of actual risk to the personal data transferred.

Question	Response
A: Assessment of inherent risk	
Taking into account the responses at Section 1 above, what is the overall inherent risk level of the data protection rules of the third county?	High. Although there are a number of data protection rules that reflect similar standards to the GDPR, there are key concerns relating to the powers of US federal agencies to access personal data (in particular where no warrant is required under FISA Section 702). These were the concerns raised in the *Schrems II* judgment and therefore indicate that an essentially equivalent level of protection may not be provided for certain types of transfers.
B: Risk assessment taking into account factual circumstances and safeguards available	
Details of the transfer	
Who is the recipient of personal data in the third country?	Google is the recipient of personal data. Google is a cloud service provider and provides hosting services to TfS. For these purposes, personal data is hosted in the US.
What personal data will be transferred to the third country and who are the data subjects?	The personal data transferred to the third country can broadly be broken down into the following two categories: **Account data**: This is information that TfS requires in order to allow users to set up an account with Book Creator. This includes name, email address, password and school. This also covers technical information about the use of Book Creator and other information that users choose to send to Book Creator, for example by email. Book Creator offers the option for users to sign in using their own Google or Office 365 account, in which case Book Creator receives only the user's full name and profile picture from the relevant account provider. Data subjects will be users of Book Creator. **Book data**: This includes any book content uploaded by users that constitutes "personal data". TfS does not control this and it is entirely up to the relevant school and the relevant user what information

	they upload to their books. This could include personal data if it includes, for example, text that includes information about the user or another individual from which they can be identified, photos or videos showing individuals, or audio files that include information about individuals. Data subjects could be any individual about whom a user uploads information as part of book content Generally speaking, the personal data hosted in Google Cloud will therefore be very low-risk. The impact on individual users of this personal data being hosted in the US is likely to be minimal (if any). As Google in the US never acts as controller, Google is required to act on TfS's/the school's instructions and all GDPR rights and obligations can be fulfilled by TfS and/or the school. TfS does not intend any special category personal data or other sensitive personal data to be processed. There is a possibility that this type of data could be included within book data; TfS is unable to control what book content is uploaded. Schools should be made aware of the possibility that personal data (especially more sensitive personal data) could be uploaded as book content by a pupil and that they, as controller, should always make sure they are comfortable with the topics chosen and content uploaded. If the teacher has concerns about particular content being uploaded, they should be responsible for ensuring that the content is not uploaded. Teachers should manage this with their classes to ensure that personal data uploaded as book content is as limited as possible.
What are the respective roles of TfS and the third country recipient?	In respect of account data, TfS is the controller and Google is a processor. In respect of book data, the relevant school is the controller, TfS is a processor and Google is a third party (sub-)processor. The school is the controller because each teacher will decide what topics or content should be included in books created by their class and, therefore, has control over whether the topic or content will require personal data to be uploaded as book content. For example, a teacher may decide to ask pupils to create an "All About Me" book which could include extensive personal data about the individual child (as well as about other individuals, such as family members or friends). TfS has no control whatsoever over this and simply provides the platform to enable pupils to create books. Schools should be aware of the possibility that book data could include personal data and should ensure that they are happy for any personal data that might be included in book content to be uploaded and hosted in Google Cloud in the US. In line with the data minimisation principle, personal data in book content should be minimised as far as possible.
What is the nature and purpose of the transfer?	Account data is stored in Google Cloud in the US in order to allow TfS to enable users to set up and log into their Book Creator accounts, as well as for TfS to manage those accounts and respond to queries or other communications from users. Book data is processed for the purposes of allowing school children to create and publish their own e-books including content created by them and prescribed by the relevant school/teacher.

Compliance with other key data protection requirements	
Are data subjects made aware of how their personal data will be processed and the transfer to the Third Country?	Yes. TfS provides a detailed privacy notice for non-US users which is available here.
Is there an appropriate lawful basis for the processing of personal data? Is the transfer of the data fair and lawful?	Yes. Where TfS is a controller (in relation to account data), there is a contract formed between TfS and each user for the provision and use of the Book Creator application and the processing of the data is necessary for the purposes of fulfilling this contract. Where TfS is a processor (in relation to book data), the school is responsible for determining the appropriate lawful basis. The transfer of the data has a minimal impact on individuals and is therefore fair and does not contravene any legal requirements.
Is the processing of personal data by the recipient in the Third Country limited to specified and lawful purposes?	Yes. Google is a processor on behalf of TfS and therefore is only entitled to process the personal data on TfS's instructions. The only purposes of the processing are as set out in the privacy notice above and Google's processing as a processor falls within these purposes.
Is the data that is transferred to the Third Country adequate, relevant and limited to what is necessary?	Yes. Account data is limited only to what is strictly needed in order for TfS to provide and run users' accounts and is very minimal in nature. TfS does not control what book data is uploaded but schools and users will be able to make sure that the content they upload does not include excessive personal data.
Is personal data that is transferred to the Third Country accurate and, where necessary, kept up-to-date.	Yes. All account data is provided directly by the user. Book data may, by its nature, be fictional (in which case it would not be "personal data") or include opinions.
Are there appropriate technical and organisational measures in place to ensure a level of security appropriate to the risk of the processing of personal data?	Yes. Google provides robust security measures to protect data stored and processed in Google Cloud. Detailed information is available here.
Is the personal dta kept in an identifiable form for no longer than necessary for the purposes of the processing?	Yes. Account data and associated book data is deleted when the account is closed.
If the importer is a processor, is there a contract in place that includes all mandatory clauses required by data protection legislation?	Yes. Google's standard data processing and security terms apply.
Applicability of problematic rules to third country recipient	

Is the third country recipient subject to specific laws requiring them to provide personal data to public authorities on request?	Yes. Google is a “remote computing company” and will therefore fall within the definition of an “electronic communications service” provider for the purposes of FISA Section 702. This means that Google will be under the FISA obligations to facilitate the bulk collection of personal data about multiple individuals without a need to show probable cause and without informing the relevant individuals. However, the Foreign Intelligence Surveillance Court (**FISC**) supervises whether individuals are properly targeted under Section 702 FISA and the government is under obligations to record the reasons for targeting a specific person. Targeting procedures are approved annually by the FISC and governmental access to personal data under FISA Section 702 is limited to the particular purpose(s) approved by the FISC. Individuals also have redress for violations of Section 702 FISA. FISA itself allows individuals who have been subject to FISA surveillance and whose communications are used or disclosed unlawfully to seek compensation. There are other avenues for redress under the Electronic Communications Privacy Act and the Administrative Procedure Act. FISA contains a number of other safeguards, including: a) the government must submit its querying procedures, targeting procedures and minimisation procedures to the FISC every year to obtain its annual FISA Section 702 certification; b) requirements for agencies to maintain Privacy and Civil Liberties Officers to advise on privacy issues and ensure there are adequate procedures to receive, investigate and redress complaints from individuals; and c) disclosure and reporting requirements, e.g. to provide annual good faith estimates of the number of FISA 702 targets. EO12333 does not compel Google to provide personal data in any circumstances.
If yes, does the third country recipient publish information about the number of such requests it receives?	Yes. Google publishes a transparency report that is regularly updated and that shows the number of FISA requests received and the number of accounts affected. Taking into account Google’s size and the number of accounts held with Google globally, the numbers of requests and accounts affected are relatively small.
Could the recipient, by virtue of its business industry, be a primary target of investigations or information requests by the public authorities of its country?	Yes. Google is an electronic communications service provider and is likely to hold information about a significant number of individuals globally. Therefore, in the event of a particular individual being targeted under FISA, Google would be a likely target of a request for information.
Likelihood of third party access to personal data transferred	
How likely is it that a third party will access the personal data transferred to the recipient?	Very unlikely. Although Google is subject to FISA, the risks of Google receiving an access request for account data or book data are extremely low. The nature of the personal data is unlikely to be something that would

	interest US government agencies. In order to be the subject of a FISA request, the user would have to be a particular target of the US government, with such targeting approved by the FISC. Therefore, although Google is subject to FISA and does receive a limited number of FISA requests (taking into account the volume of data processed by Google), the risk of Google receiving any FISA request requiring Google to allow access to account data or book data is negligible.
Risk of harm to data subjects if access were to occur	
What is the risk of harm to data subjects if a third party did gain access to the personal data?	Very low. The nature of the data is very low-risk as it consists only of basic account details (for account data) and only any personal data that the user chooses to upload (for book data). The individuals concerned are extremely unlikely to be the subject of any FISA request and even in the highly unlikely event that they were, Google could only make available very limited personal data that would have minimal impact on the data subjects.
Additional safeguards offered by the recipient	
Does the third country recipient offer particular safeguards or supplementary measures to mitigate any data protection risks?	Yes. Google has extensive publicly available information detailing how it addresses the challenges raised by *Schrems II*[38]. The safeguards that Google has in place include: Encryption: Crucially, Google encrypts data both at rest and in transit and the encryption standard used is higher than industry standard. Access transparency: Google provides logs of actions taken by Google staff when accessing user data, so TfS has visibility of access by Google. Government requests for data are identified within the access log (unless Google is legally prohibited from notifying TfS of requests). Access approval: Allows TfS to explicitly approve access to data before it takes place (subject to exceptions where legally required). Processes for dealing with government access requests: If Google receives a request for TfS data, generally Google will inform the agency to request it directly from TfS. If the government refuses to do so, Google is clear that it reviews the request carefully and thoroughly to verify that it is lawful and proportionate. Google will notify TfS wherever possible of the request and will take into account any objections TfS raises to such a request. SCCs: Google has SCCs in place that apply automatically and these will be updated to reflect the new EU SCCs in due course, as well as the new UK IDTA/addendum as and when these are approved.

[38] https://services.google.com/fh/files/misc/gsuite_foredu_whitepaper_gdpr_schremsii.pdf and https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf and https://cloud.google.com/files/gcp-trust-whitepaper.pdf

	These will impose additional contractual safeguards and obligations on Google with regarding to government access requests.
C: Assessment of residual risk	
Taking into account the responses at section 2B above and in particular any mitigating factors and additional safeguards/supplementary measures available, what is the residual risk of the relevant transfers?	Low. Although US surveillance laws have been identified by the CJEU as potentially problematic and those laws do apply to Google in its capacity as a cloud service provider, the practical chances of Google being subject to any request to disclose account data or book data to any US government agency are extremely low. The main reason for this is that account data and book data relating to teachers and schoolchildren in the UK and the EU, processed for the purposes of providing an educational book creation and publishing tool, is exceptionally unlikely to be of any interest to US government agencies. FISA contains clear protections around the targeting procedures used by US government agencies and these must be signed off annually. This means that non-US individuals will only ever be targeted where such targeting is reasonable, proportionate and justifiable. Given the relatively small number of requests received by Google (relative to the number of accounts and users and the volume of personal data processed by Google), it is very unlikely that any of these requests would be targeted towards account data or book data. It is even more unlikely, given Google's standard process to try to redirect requests, or if that fails, to notify TfS of requests and take on board TfS's objections, that access would take place without TfS being aware of, and having some level of control over, such access. Though these are therefore theoretical risks, our view is that in practice the possibility that these risks could arise is negligible. Even in the highly unlikely scenario that these risks did materialise, the risk of harm to the relevant data subjects is extremely low. Account data is extremely limited and only includes basic user details. Users are fully in control of what book data they upload and are able to make sure that they only upload information they are comfortable including. Schools and teachers can further control this by setting appropriate topics and ensuring that users do not input excessive or sensitive personal data. Furthermore, Google offers a range of strong technical safeguards, including encryption in transit and at rest, to ensure that personal data is protected from unauthorised third party requests. Taking all of the above into account, our view is that in relation to the transfers currently envisaged, no additional supplementary measures are required to be put in place. It is worth noting that TfS is looking to move data to UK or EU servers as soon as this is commercially practicable.

tltsolicitors.com/contact

Belfast | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus