Manual Guidance

Introduction

Welcome to the UK's Data Adequacy Assessment Manual. You will be using these documents to gather information to inform decision-making - by the Secretary of State for Digital, Culture, Media, and Sport - as to whether a country[1] provides 'adequate' levels of data protection according to UK law.

The UK is pursuing an outcomes-based approach to assessing adequacy, considering the overall effect of a third country's data protection laws, implementation, enforcement, and supervision. Protections in a third country do not need to be identical to those in the UK.

You will use the Manual documents to provide a broad range of information on a third country's laws and practices by answering questions in the **Template** document. This **Guidance** is intended to assist with this process by highlighting certain concepts or material that we expect to be relevant, providing some context as to why we are asking certain questions, and explaining what *we* in the UK mean when we use certain terms. However, you should not treat this Guidance as a strict 'how-to' guide: each country does data protection differently, and there may be relevant material or concepts which we have not explicitly captured in this Guidance. Please use your own professional expertise and judgement and seek further advice from appropriate sources as may be necessary.

By adopting a systematic approach to evidence collection with clear and consistent themes, we are not only building an efficient process but also one that will provide organisations with the information they need to compare and contrast jurisdictions globally. On making adequacy regulations in respect of given countries, we will publish the populated Manuals such that this body of knowledge can serve as a useful reference point on data protection laws worldwide.

NB. The Assessment Manual and associated Guidance document are intended as a guide to inform, direct, and empower adequacy assessment work. As the UK adequacy assessment capability matures and more country assessments are conducted, the guidance will necessarily evolve and iterate to reflect the lived experience of assessing adequacy.

[1] 'Country' being used as shorthand for the country, territory or sector within a country, or international organisation being assessed for adequacy. Legal specifications can be found in sections 17A and 74A of the UK Data Protection Act 2018 and Article 45(1) of the UK General Data Protection Regulation.

What to include

A description of laws and practices that are relevant to the level of data protection in the third country.

This should include information relating to the **content of relevant laws**, for example:

- A dedicated cross-cutting or 'comprehensive' data protection law;
- Other laws and practices that regulate the use of personal data such as laws relating to privacy more generally, or laws which apply in specific contexts such as employment, financial services, or the protection of public safety.
- Exceptions, exemptions and limitations to the protection of personal data, including whether and what alternative protections exist in such instances, including whether and what alternative protections exist in such instances.
- The extent to which local laws apply to UK data subjects and personal data transferred from the UK to the third country (and beyond).

This should include information on the **effectiveness of relevant protections** (i.e., how protections work in practice, or 'on the ground'), including:

- How relevant laws work within a country's broader legal framework (e.g., the relationship to broader privacy rights and whether / how courts or other administrative bodies interpret or apply relevant laws).
- Evidence of enforcement (e.g., by regulators, courts, and/or other administrative bodies). This evidence can be qualitative (such as case law or third party commentary) or quantitative (such as records of enforcement by regulators, or number of successful and unsuccessful challenges in court).
- Reports published by third party organisations (e.g., studies and surveys on public attitudes to and/or use of privacy protections), with appropriate context (see below).

While some sections of the Template specifically call for some of the above information - for example, Section 3 particularly focuses on enforcement - you should consider all of these points as you fill out each section.

How to present the information

Please provide summaries of key points, with clear references which can help officials and Ministers read the referenced material as required. We are not expecting full reproductions of all material, but key points should be drawn out.

> *For example*: "Section 1 of the Data Privacy Act provides definitions of 'personal data', 'data collection', 'privacy protection officer', 'privacy guidance'. For this section the most relevant are 'personal data' and 'data collection', which are defined as [...] and [...] respectively."
> "Section 10 of the Data Privacy Act introduces the "Right of Access", which is defined as [...]. There are exception to the application of this right, which are [...]"
>
> "Section 10 of the Data Privacy Act introduces the "Right of Access", which is defined as [...]. There are exceptions to the application of this right, which are [...]."

You should not be providing your personal views, but you should use your expert judgement to provide a complete and balanced account of the relevant information, and **its relevance to protections and rights of UK data subjects in the context of cross-border transfers**.

When commenting on evidence of protection in practice, please give an indication as to what the evidence suggests about the effectiveness of enforcement (including by court(s) and/or regulator(s)). You should be objective and balanced in this commentary, and be clear when you are providing your own expert judgement.

> *For example*: 'In the case *Defendant vs. Regulator 2016*, the court ruled in favour of the defendant that the regulator had taken an overly narrow interpretation of 'privacy'. Legal commentary on this case suggested the regulator was not fulfilling the responsibilities intended by the Privacy Act. The regulator has since published clarificatory materials on interpreting 'privacy'. In subsequent cases (*Complainant vs. Regulator 2018, Plaintiff vs. Regulator 2020)* the courts have ruled in favour of the regulator. In our view this suggests that the regulator has responded to these complaints and is fulfilling the responsibilities intended by the Privacy Act.'

Some of the evidence you provide may not be 'neutral' - material from the regulator's website, or from privacy groups, for example. Please consider this material and provide relevant context that helps the reader understand its usefulness.

> *For example:* 'The regulator and a non-governmental organisation (NGO) have published conflicting reports on new legislation. The regulator has previously been accused of being overly pro-government, but since the appointment of the new director they have frequently criticised the government. The NGO has successfully brought cases on three occasions (and unsuccessfully on one occasion).'

Some of the evidence you collect may fit in multiple sections; if so, please consider carefully which section it fits in best to aid the reader. You may cross-reference to previous sections, and also to upcoming sections, as appropriate; however, **it may often be most useful and coherent to replicate the most salient information in each section to which it applies**.

1. Terminology

The below are terms used in the UK Data Protection Act 2018 and the UK GDPR. We define them here in case it assists in understanding terms used in the Template - **but we note that an absence of these terms, or comparable terms, in other countries should not be read as an absence of adequate protections.**	
Personal Data	Any information relating to an identified or identifiable natural person ('a data subject').
Data Subject	An identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special categories of personal data	Personal data which, because of its sensitivity, may pose a particular risk to Data Subjects when processed and needs enhanced protection. For example, under the UK GDPR, special categories of personal data are defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data where it is processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The UK GDPR also imposes additional safeguards for the processing of personal data relating to criminal convictions and offences or related security measures. Some countries may provide enhanced protection for other categories of personal data, such as financial data or the data of minors.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, preservation or destruction.
Controllers and processors	Controller refers to a natural or legal person, public authority, agency or other body that determines the means and purposes of processing the personal data of others. A processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller.

2. Evidence-gathering

- The sections listed below correspond to those in the Template.

- The additional details set out here are provided as a **guide** to areas we would expect to be taken into account within this part of the assessment. **They are not intended to form an exhaustive or prescriptive list of matters to assess, and you must take into consideration other factors which you believe to be relevant to the country's data protection regime.**

Contents

Executive Summary

Please summarise key findings from the sections below.

1. Domestic & International Context

1.1	Domestic & International Context

1.1(a) Summarise relevant details about the legal and political structure of the country/sector/territory

This section is important in providing an introduction and contextual overview of the country/sector/territory.

Relevant details might include:

- Constitutional framework and/or relevant legal ties to other countries - e.g. if a country is a dependent territory of another state - and how these relations work. This is particularly important if assessing a territory/sector within a country as we need to understand ways in which data protection within the sector/territory is dependent on, or independent of, the broader country.
- Information about the political structure of the country, such as whether it has a separate and independent executive and legislature; and any potential developments, such as upcoming elections or reforms, which could impact on data protection law.
- The structure of the legal system, including how independence of courts is ensured (and any evidence of whether this is effective in practice).
- Ability of individuals (including foreign citizens) to access the court system, administrative tribunals and/or other arbitral remedies.
- Provenance of the country's legal commitment to privacy, and evidence of contemporary political commitment/recognition of value of data.
- Cultural factors which should be taken into account. For instance, is there generally a culture of strict compliance with regulations? What are general public attitudes towards privacy? Where does this understanding come from?

You should consider whether the country adheres to recognised human rights within its overall legal framework, for example:

- Protection from unnecessary and disproportionate interference with privacy;

- Rights to a fair trial;
- Freedom of expression, association, and peaceful assembly;
- Prohibitions on arbitrary arrest and detention; and
- Prohibitions against torture and cruel, inhumane, or degrading treatment or punishment.

It may be helpful to review and consider any publicised cases / commentary that may indicate whether the country does or does not adhere to international human rights. In this context you may find it helpful to consider commentary from prominent human rights groups, reports from international organisations such as the United Nations, or relevant cases or international proceedings involving the country at recognised human rights fora (e.g. ECHR).

1.1(b) Has the country signed up to and/or ratified international conventions relating to privacy and/or data protection? If yes, provide details. To what extent does the country participate in international organisations or systems promoting privacy and/or data protection? Also include regulator network participation.

Examples include, but are not limited to:

- The Universal Declaration of Human Rights (UDHR)
- European Convention on Human Rights
- EU Charter of Fundamental Rights
- Convention 108 and/or Convention 108+
- Treaty of Rome
- Global Privacy Assembly
- Asia Pacific Privacy Authorities (APPA) Forum
- Organisation for Economic Co-operation and Development Privacy Framework
- Madrid Resolution on international privacy standards
- European Data Protection Board
- APEC Privacy Framework Standards for Personal Data Protection f American States
- African Union Convention on Cyber Security and Personal Data Protectio
- ECOWAS Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

You should:

- Obtain confirmation of which relevant international treaties have been adopted, including details of when the relevant treaty was ratified and the extent to which the obligations are enforceable and have been enforced in practice.
- Review evidence of implementation of treaty principles through the drafting of relevant local law.
- Review evidence of treaty obligations being complied with and/or enforced through judicial, administrative and supervisory enforcement action.
- Provide any relevant evidence as to whether the country follows and/or actively participates in these international commitments / organisations.

1.1 (c) Do any bilateral or multilateral agreements (e.g. trade deals) impose requirements on the country regarding privacy and/or data protection? Look at data flows as part of international trade agreements, in particular the digital chapters, which may provide information on how the jurisdiction provides for onward transfers. ● For example, do any trade deals include data localisation requirements (e.g. that companies store data, or copies thereof, in a specific country)?
Any additional information or comments?

2. Domestic Laws and Rules

Please take the following into consideration:

- Legislation with relevance for protecting personal data
- Professional rules / codes of conduct / self-certification
- Effects of international commitments
- Other legally binding means of protection
- The territorial scope of these protections, in particular whether they apply differently to foreign nationals, citizens, or residents, etc.
- Any exemptions from rules and laws

2.1	Laws and Scope

General considerations:

- When considering the level of personal data protection provided under a country's laws, it is important to describe the key concepts used in the relevant legislation. For example, does legislation use concepts such as 'personal data', 'personal information' or similar? If there is no single, pervasive definition of personal data within the legislation itself, are there other ways of defining such a concept?

- It is also important to ensure that any exemptions are appropriately captured. For example, does the definition of personal data regulated by law exclude certain categories of data which relate to an individual? In some countries, protection is only provided for specific sets of data, such as financial data or health data, rather than a broader concept of personal data used in English law.

2.1(a) What laws and rules exist which govern the collection and use of personal data?

For all other questions, 'data protection legislation' will be used as a shorthand for these laws and rules.

Many countries regulate the processing of personal data within a single data protection law. You should identify whether such a law exists and consider its scope, as many data protection laws include limitations which may exclude certain persons, organisations or territories from coverage.

- For example, in some countries, only organisations over a certain size (based on annual turnover, or workforce) are subject to data protection legislation;

or public sector organisations may be regulated by different legislation to commercial entities.
- Some laws make provision for extra-territorial effect.

Alternative personal data may be protected through provisions contained in multiple laws and regulations of the country.

- Are there industry specific laws regulating healthcare providers, financial institutions, e-commerce businesses, which when taken together provide a comprehensive framework?
- Are certain types of processing (law enforcement, national security) covered through a separate legislation or covered through exemptions in the general data protection law?
- Do other laws or binding codes of conduct have the effect, when taken together, of creating a legally binding data protection framework? For example, equivalent legal protection may exist in constitutions, regional or state level legislation, industry or sector-specific legislation, overarching human rights law or binding industry codes of practice.

2.1(b) To whom does the data protection legislation apply? Please include a description of any exemptions or types of organisations that are treated differently, and if so, how the treatment differs.

Please include in this section any requirements and/or exemptions specific to public authorities, and agencies tasked with law enforcement, national security, and/or defence.

It is important that you consider:

- What laws regulate the processing of data by authorities which carry out tasks in the public interest. Are these authorities regulated differently to bodies that process data for other purposes? In what situations can these authorities access personal data?
- What laws regulate the processing of data by authorities tasked with law enforcement, national security, and/or defence. Are these authorities regulated differently to bodies which process data for other purposes? In what situations can these authorities access personal data?
- Whether there are any substantive or procedural requirements that apply to these authorities regarding their collection and processing of personal data; for example, does the law require that personal data should be accessed and/or stored by public authorities only where it is necessary, justified and proportionate to do so?
- Whether the laws contain any limitations, safeguards or oversight on these authorities' access to and retention of personal data; for example, consider the extent to which any collection and retention of personal data have to be balanced against the rights and interests of the individual concerned or pursue a legitimate aim.
- Whether certain organisations or sectors are exempt from relevant legislation, or whether other significant areas not covered by legislation; for example,

in some jurisdictions, data protection obligations only apply to organisations over a certain size (based on annual turnover, or workforce), or based on the type of processing they carry out or services provided, such as operators of commercial websites/online services and telecoms.

You should also consider:

- Do laws distinguish between the role of a controller and processor? These terms may not be used, but is there a distinction in data protection legislation between the level of regulation applicable to those who take substantive decisions in relation to the processing of personal data, as opposed to service providers, vendors or other parties who process data on someone else's instructions?

- Do laws apply additional or different regulation to organisations operating in specific sectors, such as the health sector, employment sector or financial sector; or certain professions such as legal or accountancy professions?

You should consider, if necessary, providing appropriate context about key public authorities who process personal data.

- For example, are there specific public authorities who use personal data to combat particular sorts of crime? Are there multiple authorities who can use investigatory powers to collect personal data, and if so who are they and in what circumstances can they use such powers?

2.1(c) What are the categories of person to which the laws or rules afford protection to? Are there any exceptions to the groups afforded protection by the laws? Does the data protection legislation (or any other relevant rules) apply differently or exclude foreign nationals, citizens, or residents?

Categories might include, for example, natural persons, legal entities, etc.

Exceptions might include, for example, children or other vulnerable persons, people convicted of crimes, etc.

Consider whether non-domestic data subjects can exercise the rights contained within the applicable laws or whether constitutional level principles (or similar) apply to non citizens.

2.1(d) What types of personal data are covered by data protection legislation? Please include a description of any types of personal data that are treated differently, and how the treatment differs.

Are enhanced levels of protection afforded to categories of personal data considered to be particularly sensitive and the processing of which is considered to be particularly risky? If so, how are these categories defined and what additional protections apply?

- For example, legislation may require there to be specific legal grounds in place before special category personal data can be processed; employment legislation may restrict the processing of criminal offences data; or specific health sector legislation may restrict the processing of health data.

Consider whether there are any limitations on the types of personal data sets covered by the laws (i.e. are there categories of personal data that are not caught by data protection laws?).

2.1(e) What types of processing of personal data are covered by data protection legislation? Please include a description of any types of processing which require lower or enhanced protections, explicit or implied prohibition of specific types of data processing.

Are any types of processing of personal data exempt from regulation?

- For example, some countries only regulate the processing of personal data by automated means (i.e. processing which is carried out using a computer, mobile device, router etc.) but not processing of manual records / paper files, or processing for purely household purposes.

Consider whether there are restrictions on processing activities that may be seen as more invasive, and therefore higher risk for individuals.

- For example, are there special regulations which apply to video surveillance, facial recognition, automated profiling, and/or data mining?

2.1(f) Does data protection legislation require the prior identification of lawful purposes or reasons for the processing of personal data and are any purposes treated differently (and if so, how)?

Please include in this section any specific requirements and/or exemptions which apply to personal data processed for law enforcement, national security, and/or defence purposes.

Does the data protection legislation (or any other rules) require the prior identification of a lawful basis for the processing of personal data? The lawful bases could include, for example, that the processing is necessary for performance of a contract, required to comply with a legal requirement, or that the individual whose personal data is being processed has given their consent.

Consider whether the data protection legislation (or any other rules) require processing of personal data to be done only for specific, well-defined purposes, or whether processing of personal data can be carried out for undefined and/or unlimited purposes. Requiring processing to be carried out for a specific, defined purpose is connected with transparency, predictability and user control, and can help to enable Data Subjects to effectively exercise their rights, such as the right to object to processing. For example:

- Are there controls in place to prevent the processing of personal data in a way that is incompatible with the original purpose it was collected for?
- Are there any requirements to ensure that the purpose of processing is sufficiently specific and clear and that individuals know what to expect in relation to the processing of their personal data?

Purposes which are treated differently might include, for example:

- Additional restrictions for the processing of personal data for marketing purposes, such as email marketing and personalised online marketing? For example, can marketing communications only be sent to those individuals who have consented to receive them, do marketing communications have to contain an opt-out method, and are there restrictions in relation to the volume of marketing or marketing channel?
- Requirements or exemptions from where personal data is processed for scientific/historical purposes - such as processing in the process of carrying out scientific research, conducting health studies in the public interest etc. and carrying out historical research such as research for genealogical purposes etc.), archiving purposes
- Producing records which are of public interest, e.g. for journalism.

Any additional information or comments?

For example:

- Are there any other significant exceptions in the country relating to the scope or application of the data protection legislation?
- What are the implications of protections that do or do not exist?
- Are there plans for future legislation? If so will this include any significant changes in relation to the scope and application of data protection legislation in the country?

2.2	Protections during Processing

2.2(a) Are there any restrictions or requirements in the data protection legislation with regard to sharing personal data to other parties (within the jurisdiction),

including the transfer of personal data to, or the appointment of, processors?

Consider the extent to which the data protection legislation (or any other rules) impose restrictions and/or requirements in relation to transfers of personal data to parties *within* the country.

Consider the extent to which the data protection legislation (or any other rules) impose restrictions and/or requirements in relation to the use of party service providers to process personal data.

- For example, does the law require certain contractual provisions, particular policies, specified physical, environmental and logical security measures, regular audits and/or training for personnel to be in place when engaging a party to process personal data?

Is there any variation within the country's implementation of the data protection legislation?

- For example, do local entities (states, councils, etc.) have different tasks or powers in regards to data transfers?

2.2(b) Are there any requirements in the data protection legislation in relation to ensuring that personal data is kept accurate and up-to-date?

2.2(c) Are there any restrictions on the volume of personal data that is processed?

- For example does the processing of personal data have to be limited to a set amount of information that is directly relevant for the specific purpose pursued by the processing?

2.2(d) Are there any restrictions on how long personal data can be stored and/or processed?

- For example, are there any requirements that personal data is only processed for as long as it is necessary to fulfil the purpose of processing? Are there any requirements that personal data be deleted when it is no longer required?

Any additional information or comments?

2.3	Security, Sanctions, and Redress

General considerations:

It is important to consider the extent to which the country has a means of enforcing those laws which protect individuals' privacy and/or personal data. Consideration of these factors will assist in reviewing and interpreting the approach to regulatory supervision, rights of redress for individuals and the extent to which sanctions and penalties exist

Where the data protection legislation does not include specific requirements in relation to security or does not include sanctions or penalties for breaches of the data protection legislation, consider whether data protection legislation and privacy protections are enforced through other laws and regulations, for example, through sector specific regulations.

2.3(a) Does data protection legislation require measures to mitigate security risks to personal data, such as accidental disclosures, to be implemented?

You should consider, for example:

- The extent to which the data protection legislation (or any other rules) require security measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- The extent to which the data protection legislation (or any other rules) require security and confidentiality controls (e.g. encryption of personal data, pseudonymisation of personal data, the ability to ensure the ongoing confidentiality of processing systems and services etc.) to be implemented. For example, consider whether prescribed security measures need to be in place when processing certain sensitive categories of personal data?
- The extent to which the data protection legislation (or any other rules) require differing security measures depending on the type of personal data being processed. For example, where special categories of personal data are processed, are additional security measures required?

2.3(b) Does data protection legislation specify penalties and/or sanctions for a failure to protect personal data?

Examples might include fines, imprisonment, or revocation of a license.

Penalties might be applied to individuals, but may not - they may apply to, for example, businesses or organisations.

2.3(c) Does data protection legislation provide individuals with rights over their personal data? If so, what do these rights consist of, and are there any limitations on these rights (including any rights to appeal, and rights to participate in proceedings)?

Please include in this section any mechanisms by which individuals can seek redress for infringement of rights by public authorities.

Consider the extent to which the data protection legislation (or any other rules) require information about any proposed processing of personal data to be provided to individuals.

- For example, must individuals be provided with information about what personal data is held about them, the purpose of processing that personal data and the rights that they have in relation to their personal data?
- If so, do the transparency obligations provide individuals with sufficient information to understand what personal data is being processed, who is processing it, the purposes for processing etc.?
- Does the law set out specific requirements as to how transparency information must be provided, e.g. must it be provided in a clear and easily accessible format?

To what extent does the data protection legislation (or any other rules) give data subjects a right of access to their personal data? For example, the extent to which:

- Data subjects can request their personal data from a controller.
- Data protection legislation (or any other rules) provide individuals with the right to object to the processing of their personal data.
- Data protection legislation (or any other rules) provides individuals with the right to request that their data be corrected/rectified or erased.

If data subject rights exist, to what extent can they be exercised in practice? For example, can individuals exercise rights free of charge or do they carry a large fee? Are there timescales to respond to rights requests?

2.3(d) Are the processing activities of public authorities, including for purposes of national security, defence, and/or law enforcement, subject to review and supervision under domestic legislation? Describe the nature of any such review and supervision.

You may wish to refer back to your answer in 2.1(b), in relation to how the country describes ‘public authorities’ or equivalent.

Does the law:

- Provide for regular reviews of the terms of processing by public authorities? If not, does the country carve out exceptions to prior review and if so consider whether these are justified?
- Require processing of personal data by public authorities to be overseen by a regulator or similar body?
- Contain redress mechanisms available in relation to the access to and retention of personal data by public authorities? For example, this could include access to personal data held by public authorities for data subjects, recourse to an independent complaints panel for data subjects or recourse via the judicial system to hold public authorities' processing activities to account.

Consider whether there are any publicised cases in which it has been alleged that public authorities have violated applicable laws relating to processing of personal data. For example, you may find it helpful to consider public commentary, reports from international organisations such as the United Nations or relevant case law

2.3(e) Are there references in data protection legislation, or any other rules to any other processes which must or can take place in the event of a breach of data protection legislation, which are not already covered in previous questions?

2.3(f) To what extent does the data protection legislation (or any other rules) require and/or encourage demonstration of compliance with the laws (e.g. through a maintained record)?

For example, is there any requirement to maintain internal records of processing, notification of data breaches, appointment of a data protection officer or similar role, etc.?

Consider the existence of transparency requirements - see 2.3(c).

Consider the extent to which there are requirements to adopt governance and accountability controls within the organisation to regulate use of data.

Any additional information or comments?

For example:

- Industry practice – do relevant industries generally comply with data protection legislation? Are there industry groups with a data protection focus or industry market practice which includes data protection protections.

2.4	International Transfers

2.4(a) Are there references in the data protection legislation to restrictions and obligations on transfers of personal data outside the country (i.e. cross-border transfers, including onward transfer of UK data)?

Does the law require the transfer of data, outside of the country, to be subject to binding rules (including contractual rules) or approvals that ensure certain standards of protection are maintained and that rights of data subjects are not undermined?

Are there any variants for different types of data, types of processing, purposes for transfer, senders, recipients, and/or other distinctions? How is compliance monitored and are there specific penalties for non compliance with such rules?

2.4(b) Can personal data be transferred 'freely' (i.e. without any further safeguards) to any specified countries, territories or one or more specified sectors within a country, and/or international organisations? If so, provide details (including the grounds on which these specified countries, sectors etc. are chosen and any assessment process).

It may be helpful to consider the test/benchmark used for decisions to allow free-flow of personal data, and whether there is any guidance on deciding if the test/benchmark is met.

2.4(c) Are there any permitted exceptions to the mechanisms outlined in 2.4(a) and (b) above?

Are permitted exceptions restricted to a limited range of circumstances and are they necessary and proportionate?

Any additional information or comments?

For example, consider:

- Any case law in which transfer mechanisms have been challenged;
- Any proposed new transfer mechanisms or proposed updates to current transfer mechanisms which are not yet in force.

2.5	Additional Information
2.5(a) Are there any exemptions to the data protection legislation not already covered in previous questions (relevant to the protections and rights of UK data subjects in the context of cross-border transfers)? For example, are there exemptions to data processed within a certain time period?	
Any additional information or comments?	

3. Supervision and Enforcement

Please take the following into consideration:

- Sectoral data protection legislation / professional rules / codes of conduct / self-certification
- Case Law
- Information and guidance supplied by regulators
- Commentary by third parties

3.1	Supervisory Authority
General considerations: Consider whether a regulator function is provided by a single regulator, or whether certain sectors or territories have regulators who perform this function. For example, ● a country may not have a single national authority but instead enforce data protection legislation through a number of sector specific laws through various regulators; ● a country may have sector-specific regulators in the healthcare, financial services, telecommunications and insurance sectors, who have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.	
3.1(a) Which body or bodies (if any) regulate and/or enforce data protection legislation? Does the country have an authority (or authorities) who is able to act on data subject complaints and also investigate of its own accord? You should include any authorities tasked with oversight of public authorities' access to, and/or use of, personal data.	

3.1(b) What responsibilities and powers do these bodies have in relation to enforcing data protection legislation? Consider whether the authority has clear/ascertainable and legally binding powers to intervene / enforce compliance, including the power to engage in, initiate or provide information or mechanisms to begin legal proceedings relating to violations of the data protection rules. ● For example, does the authority have the ability to hear and/or triage claims lodged by data subjects concerning their rights?
3.1(c) What resources do these bodies have (including funding and staff numbers)? How are these bodies funded? You should include commentary on whether the regulator is considered to be equipped to properly regulate data protection in the country.
3.1(d) What is the status of the(se) authorities – i.e. to what extent are the authorities independent from the government or able to act with independence and impartiality in performing its duties and exercising its powers? Does the government have any role(s) in deciding funding, choosing staff, setting remit and powers, etc.? Are there specific rules in place which limit the ability of the government to affect the authority's activities or decisions? Is there evidence of whether the authorities are independent (or not) in practice?
3.1(e) Does the supervisory authority issue specific guidelines or recommendations, either of general nature or for specific types of data/processing, to promote compliance with data protection legislation? It may be helpful to consider whether the authority actively promoted privacy compliance. In some countries, there may not be a single data protection law but the authority may be active in issuing guidance and best practice which provide a similar level of protection. Are these guidelines issued by the supervisory authority of its own accord, and/or are they commissioned by other bodies (e.g. by sectors)?
3.1(f) Are there any arrangements and/or obligations in place regarding co-operation involving multiple supervisory authorities, or other bodies with responsibility for processing and/or protecting personal data? (This includes co-operation with bodies in countries, sectors or territories within countries, and international organisations). It may be helpful to consider whether the authority can cooperate / communicate with other regulators for cross-border investigations and enforcement.

Any additional information or comments?

3.2	Evidence of Enforcement

General considerations

Consider whether the authority has a proven track record of using its enforcement powers. For example, the law in one country may provide for enforcement powers but these may be rarely or never used.

Also consider the role of other bodies, particularly courts, in enforcing data subjects' rights.

Information-gathering should include:

- analysis of specific case law (milestone decisions), to assess whether and to what extent the authorities responsible for the enforcement follow the laws, whether the laws are extensively or restrictively interpreted etc. This includes the frequency and effectiveness of appeals against enforcement action taken and judicial decisions;
- statistical analysis of the enforcement measures (number and amount of fines / judgements, how the proceedings start on a general basis etc.); and/or
- other evidence about the enforcement regulation (assessment of general rules and efficiency of enforcement, rights of the parties, procedural rules etc.).

Evidence can, amongst other things, draw on from actual enforcement decisions, civil courts, criminal courts, appeals, administrative authorities, the data protection authority or other sources.

3.2(a) Is there evidence that enforcement of breaches of data protection legislation is independent, effective, and fair? Consider the volume and value of fines and other sanctions.

Consider whether and when enforcement action is taken by the supervisory authority and courts, including whether court judgements are enforced in practice within the country as this may be an indication of the means of enforcement and redress for individuals.

Is there evidence related to the supervisory authority's independence from the government?

- For example, has the supervisory authority ever acted against the interests of the government, or always acted in favour of the government?
- You may wish to refer to your answer to 3.1(d).

3.2(b) What evidence is there regarding the extent to which individuals can access redress for personal data breaches and/or exercise rights over their personal data (for example, by successfully lodging complaints with the supervisory authority/ies, the courts, or other administrative bodies)?

Can individuals go to the authority or court to exercise their rights and get compensation or other forms of redress? Can individuals easily access the authority/court process in order to exercise their data protection rights? You may also find it helpful to consider whether individuals have access to legal representation in order to exercise their privacy rights and also whether there are any cost barriers which in practice prevent individuals taking complaints to the authority or court.

You should consider:

- Whether data subjects are kept informed and participate in proceedings and how easy it is to appeal decisions that are made by the authority and courts. It may also be helpful to consider whether there are any fees that must be paid in order to lodge an appeal and, if so, whether these are excessive/act as a cost barrier.
- Whether data subjects can raise class actions and representative claims in relation to privacy complaints.
- How transparent and straightforward the process is in practice, and any potential barriers. For example, are costs involved which may limit or discourage data subjects from taking action?

3.2(c) Are there any other relevant evidence / cases demonstrating the effectiveness of enforcement, or concerns/criticisms about the effectiveness of enforcement, not covered in previous questions?

Any additional information or comments?