

Manual Template

*Please read the **Introduction** section of the Manual Guidance before completing this document.*

Contents

Executive Summary

1. Domestic & International Context
2. Domestic Laws & Rules
 - 2.1. Laws and Scope
 - 2.2. Protections during Processing
 - 2.3. Security, Sanctions, and Redress
 - 2.4. International Transfers
 - 2.5. Additional Information
3. Supervision & Enforcement
 - 3.1. Supervisory Authority
 - 3.2. Evidence of Enforcement

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.	
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.	
1.1(c) Do any bilateral or multilateral agreements (e.g. trade deals) impose requirements on the country regarding privacy and/or data protection?	
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
Summary:	
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.	
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.	

2.1(c) What are the categories of person that 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?

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.

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.

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.

Any additional information or comments?

2.2

Protections during Processing

Summary:

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?

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?

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

Any additional information or comments?

2.3

Security, Sanctions, and Redress

Summary:

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

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

2.3(c) Does data protection legislation provide individuals 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.

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

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)?

2.4

International Transfers

Summary:

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)?

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).

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

Any additional information or comments?

2.5

Additional Information

2.5(a) Are there any exemptions to the data protection legislation not already covered in previous questions (relevant to protections and rights of UK data subjects in the context of cross-border transfers)?

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
Summary:	
3.1(a) Which body or bodies (if any) regulate and/or enforce data protection legislation?	
3.1(b) What responsibilities and powers do these bodies have in relation to enforcing data protection legislation?	

3.1(c) What resources do these bodies have (including funding and staff numbers)? How are these bodies funded?

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?

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?

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).

Any additional information or comments?

3.2	Evidence of Enforcement
Summary	
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.	
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)?	
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?	