Cabinet Office

Procurement Policy Note

Guidance on data protection legislation

Action note: PPN 020

Previoulsy issued: November 2022

Updated: April 2025

Issue

1. This Procurement Policy Note (PPN) covers data protection requirements under UK GDPR, and the UK International Data Transfer Agreement (IDTA) governing the export of personal data from the UK.

2. This PPN replaces PPN 03/22 as part of the Procurement Act 2023 suite of republished PPNs. PPN 03/22 replaced PPN 02/18 and contained streamlined guidance, and updated legal clauses to take into account the UK's exit from the EU. It also includes guidance on international transfers of personal data.

Dissemination and scope

3. This PPN applies to all central government departments, their executive agencies and non-departmental public bodies. Such bodies are referred to as 'in-scope organisations'.

4. In-scope organisations should circulate this PPN widely across their organisations, and work closely with data protection/information assurance leads within their organisations on implementation.

5. This update does not constitute a change in policy or a new call for action but in-scope organisations should continue to apply any ongoing obligations set out in the provisions of this PPN. In-scope organisations do not need to repeat actions which were required upon this PPN's initial publication.

Timing

6. In-scope organisations should note the provisions of this PPN with immediate effect.

Action

7. In line with data protection law, in-scope organisations should already have identified existing contracts involving processing personal data and included in them the clauses provided in PPN 03/17, PPN 02/18 or PPN 03/22.

8. For contracts to be awarded after the issue of this PPN, in-scope organisations should use the updated clauses at Annex A to this PPN. Crown Commercial Services have made changes to overarching commercial agreements where necessary and communicated this via usual customer channels. In-scope organisations should also ensure any call-offs are suitably covered with appropriate clauses.

Key considerations

Data protection legal framework

9. The primary UK legal data protection framework is the UK General Data Protection Regulation (UK GDPR).

10. The Data Protection Act 2018 contains clarifications and exemptions to UK GDPR, and both pieces of legislation need to be read alongside each other.

11. The Data Protection Act 2018 includes, at Part 3, the legal framework for the processing of personal data for law enforcement purposes, and at Part 4, the legal framework for the processing of personal data by the intelligence agencies.

12. There are also limited circumstances in which EU GDPR could apply to an in-scope organisation, where it was offering goods or services to EU citizens. In these cases, in-scope organisations must comply with both UK GDPR and EU GDPR. If this applies to your organisation then advice should be sought from your data protection team or data protection officer.

Controllers and processors

13. The UK GDPR applies to ‘controllers’ and ‘processors’.

    - a **controller** is a legal person or organisation which determines the purposes and means of processing personal data. A controller is the organisation in control of the processing of personal data, who makes the key decisions, and is usually the organisation that decides to collect the personal data in the first place. It will also typically determine the specific personal data to be collected, held or used, and the appropriate legal basis of the processing, as well as how long the data will be processed, and who the data shall be shared with.

- a **processor** is a legal person or organisation which processes personal data on behalf of a controller. A processor will not be responsible for making the key decisions about the personal data and will only be processing the data under the direct, or implied, instructions of the controller. Therefore, the processor will not be processing any of the controller's data for any of its own purposes, and has no direct interest in the data itself. The processor may be providing its expertise to the controller in respect of technical or other matters, and may have scope to make some decisions about the manner in which personal data is processed, but only to the extent that the contract with the controller allows.

14. A controller-processor is likely to be the appropriate relationship in the vast majority of buyer-supplier relationships. In most cases in public sector contracts, the public body letting a contract or calling-off from a framework agreement will be the controller, and the supplier will be the processor.

15. Different legal obligations apply depending on the nature of the relationship with the supplier. Where the supplier is a processor, there is a legal obligation under Article 28 UK GDPR to have a contract with the processor and for it to contain specific data protection clauses. Part 2 of Annex A contains the clauses required by law in a controller-processor relationship.

Crown to Crown data agreements

16. Where a Crown Department acts as a processor for another Crown Department, Section 209(2) of the Data Protection Act 2018 stipulates that each Crown Department is a separate controller in law. As a matter of law, the Crown cannot contract with itself.

17. Section 209(3) of the Data Protection Act 2018 resolves this by providing that where the UK GDPR or the 2018 Act requires the relationship between controller and processor to be governed by a contract, a memorandum of understanding (MoU) will be sufficient. The MoU must include the clauses at Annex A of this PPN.

Joint or independent controllers

18. In a limited number of circumstances, a supplier may be acting as a joint controller (jointly determining the purposes and means of processing) or as a controller in their own right rather than a processor. Where you suspect that this is the case, consult your local data protection team or data protection officer for advice. In these scenarios the clauses at Annex A are unlikely to be appropriate and you should take advice from your data protection team or data protection officer on the data protection provisions you should have in place.

Cost of compliance

19. Any organisation required to comply with data protection legislation may incur costs in doing so. Suppliers will be expected to manage their own costs in relation to compliance. In-scope organisations are advised not to routinely accept contract price increases from suppliers as a result of work associated with compliance but should apply commercial judgement in individual discussions on this with suppliers.

Risks of non-compliance

20. In-scope organisations who do not comply with data protection law will be in breach of the regulations and at risk of being fined, or having an enforcement order issued against them, by the Information Commissioner's Office (ICO).

21. Under the UK GDPR, processors have direct legal obligations to comply with data protection law, and they can be fined by the ICO. Both controllers and processors can also face private claims for compensation where they have not complied with their obligations under UK GDPR.

Contract liabilities

22. In-scope organisations should not accept liability clauses where processors are indemnified against fines or claims under UK GDPR. The legal penalty regime has been extended directly to processors to ensure better performance and enhanced protection for personal data, therefore entirely indemnifying processors for any regulatory fines from the ICO or civil claims from data subjects undermines these principles.

23. As the UK GDPR gives processors responsibilities and liabilities in their own right, processors, as well as controllers, may now be liable to pay damages or be subject to fines or other penalties from the ICO. In addition to the maximum regulatory fines, the increased rights of data subjects under the UK GDPR may also lead to greater exposure to civil claims for data protection breach. In-scope organisations should consider reviewing liability and indemnity provisions on a contract by contract basis if there is a risk that they might otherwise prevent recovery of these costs. In-scope organisations should consider this in accordance with the nature of the procurement, the appetite for risk and the type of personal data involved in the contract.

24. There are a range of options to be considered, to ensure the controller is able to recover the full costs of civil data protection claims or regulatory fines issued by the ICO, where the processor is at fault, and these might include:

    - excluding all data protection breaches from the general cap on liability
    - increasing the general cap on liability to ensure it covers higher regulatory fines
    - having a separate cap on liability for all data protection breaches
    - introducing a separate £17.5 million cap on liability for regulatory fines arising out of data protection breach

25. When varying existing contracts, in-scope organisations should apply commercial judgement when considering whether substantial changes or additions to liability and indemnity clauses should be made in accordance with the change in law provisions in contracts. The existing provisions may be sufficient to cover-off the risk.

Expired/legacy contracts

26. There may be some instances where personal data is still being processed by a processor, for example it may be stored by the processor, even though the contract has expired. Data being processed in such circumstances is in breach of the legal obligation to have a contract in place where a processor is used to process personal data. It is also in breach of the data processing principles, which controllers are responsible for compliance with, as such storage is no longer necessary.

27. Without a contract, it is possible that a controller will not be meeting its obligations to ensure data security. In such circumstances you should take advice from your data protection team or data protection officer. Unless the buyer and supplier are in agreement that the necessary clauses have survived the original contract covering the data processing, it is likely that an interim contract will need to be put in place. However, this should only be a temporary measure and steps must immediately be taken to ensure that any data which it is no longer necessary to process (including storage) is returned to the controller and/or deleted.

28. These provisions will protect the data and ensure that the controller and processor agree on their roles and responsibilities. This may need to exist as a separate contract if the existing contract has already expired.

Protective measures

29. As set out in Article 28(3)(c) UK GDPR, processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and these are defined as 'protective measures' within Annex A.

30. In-scope organisations may consider using security schedules for contracts involving personal data processing, to provide a framework to ensure comprehensive assurance of a processor's compliance. Controllers may reject a processor's proposed measures if they think they are insufficient. Examples of the security considerations are at Annex B.

Data processing outside the UK

31. Article 44 of UK GDPR prohibits the off-shoring of personal data outside the UK unless a legal gateway is in place. Valid legal gateways include:

    - an adequacy decision[1] by the UK government in respect of the destination country
    - EU standard contractual clauses[2] (until 21 March 2024 if the contract was concluded on or before 21 September 2022) or the UK International Data

[1] For a list of territories granted adequacy see: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/#Q1

[2] SCCs as set out in European Commission Decision 2001/497/EC and European Commission Decision 2010/87/EU.

Transfer Agreement (IDTA)[3] between the data exporter and importer organisations

- binding corporate rules where data is exported from one part of a group of companies to another member of that group and the rules have been approved by the Information Commissioner
- a legally binding and enforceable instrument between public authorities
- transfers pursuant to a code of conduct approved by the Information Commissioner (none currently exist)
- transfers pursuant to a certification mechanism approved by the Information Commissioner

32. If your contract does involve data being offshored outside the UK, you should identify the legal gateway that the supplier is relying on to make that lawful. The most common legal gateways that you will be relying on are an adequacy decision and standard contractual clauses/IDTA.

Adequacy decisions

33. The UK government has declared that the European Union and European Economic Area (EEA) are adequate for data protection purposes. Likewise, the European Commission has also declared that the UK is adequate for data protection purposes. This means that personal data can flow unfettered between the UK and the EU/EEA. The UK and USA have also agreed a UK Extension to the EU-US Data Privacy Framework. This is a form of partial adequacy decision that applies to companies registered under the Framework.

34. The UK government has also provisionally made an adequacy decision in respect of the countries that the EU considers adequate. These include New Zealand, Israel, Switzerland, and Argentina. Limited adequacy decisions have also been made in respect of Japan and Canada.

EU Standard Contractual Clauses (SCCs)

35. Sometimes called “Model Clauses”, these are clauses approved by the Information Commissioner and UK Government that ensure protection for data by contractual means where the destination country has not been deemed adequate. Where these clauses are in place (either as part of the contract or as a separate agreement), personal data can be exported from the UK to the supplier.

36. The EU GDPR standard contractual clauses approved by the European Commission (Decisions 2001/497/EC and 2010/87/EU) were transitionally recognised as a legally valid gateway under UK GDPR, so in-scope organisations could have continued to rely upon these SCCs until 21 March 2024 if the contract had been concluded on or before 21 September 2022. In order to rely upon the SCCs, the processing operations

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

that were the subject matter of the contract had to remain unchanged and reliance on those clauses had to ensure that the transfer of personal data was subject to appropriate safeguards.

UK International Data Transfer Agreement (IDTA)

37. On 21 March 2022 the UK government commenced a new legal instrument that provides protection for personal data exported from the UK where an adequacy decision was not available. The International Data Transfer Agreement (IDTA) is essentially the UK version of standard contractual clauses.

38. The IDTA comes in two forms:

    a) A stand-alone IDTA that covers exports of personal data from the UK.

    b) A form of IDTA that "plugs in" as an addendum[4] to the EU SCCs. The second version is appropriate where data may be transferred to a non-adequate territory from both the UK and EU/EEA.

39. For contracts concluded after 22 September 2022 you must use one of the two forms of IDTA. For existing contracts or those concluded on or before 21 September 2022 you may have continued to rely on the EU SCCs, but only until 21 March 2024

The Schrems 2 case

40. In July 2020, the European Court of Justice struck down the partial adequacy decision ("Privacy Shield") made by the European Commission in respect of the USA. The court took the view that the USA's surveillance legislation was disproportionate and thus personal data could not be safely exported to the USA under that decision.

41. The court also reviewed the issue of transfers of personal data which were protected by EU SCCs. The court affirmed that EU SCCs were a valid transfer mechanism, but found that in relation to certain countries EU SCCs might need to be supplemented by additional protections in order for transfers to be lawful.

42. The ICO has published guidance[5] which asks that controller organisations consider a range of risk factors relating to non-adequate countries, including whether there are partial UK adequacy regulations in relation to that country, its human rights record, its legal and court system, and how close those systems are to the UK legal and court system, how overseas judgments are recognised and enforced; and its laws and practices regulating third parties access (including public authority surveillance). The ICO recognises that conducting such an assessment is not straightforward, and you should consult your data protection team for advice where data is to be transferred

[4] https://ico.org.uk/media/for-organisations/documents/4019535/addendum-international-data-transfer.docx
[5] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/

from or accessed from a non-adequate country.

The Law Enforcement Directive (LED)

43. Part 3 of the Data Protection Act 2018 applies in relation to domestic and cross-border processing of personal data for law enforcement purposes. Similar obligations apply as under UK GDPR, but there are some significant differences, in particular in relation to the storage and classification of data. The ICO has produced guidance on law enforcement processing.

44. Whilst the standard generic clauses at Annex A are compliant with the requirements of Part 3 of the Data Protection Act 2018, in-scope organisations engaged in processing personal data for law enforcement purposes as controllers may require more specific drafting in contracts to flow some of these obligations down to their processors. Legal advice should be sought in these cases.

Sources of further information

45. The Information Commissioner's Office is a useful source of the latest information on data protection law. Other sources of information are listed below:

    ICO Information on UK GDPR

    General Data Protection Regulations

    ICO guidance on law enforcement processing

    UK GDPR

Contact

46. Enquiries about this PPN should be directed to the Crown Commercial Service Helpdesk (telephone 0345 410 2222, email info@crowncommercial.gov.uk)

47. Enquiries on UK GDPR should be directed to your data protection team, data protection officer, or the Information Commissioner's Office (on 0303 123 1113 or via their Live Chat service, available through their website).

Annex A Part 1: Generic standard UK GDPR clauses

Notes for completion: As the standard definitions highlighted below are not specific to UK GDPR, they should be amended and adapted to fit within your existing contract definitions. The UK GDPR generic standard clauses may also be adapted to fit existing contract templates but you are advised to seek legal advice when doing this.

[STANDARD DEFINITIONS, WHICH MAY NEED AMENDING]

Customer: [to be completed as appropriate]

Contractor: [to be completed as appropriate]

Party: a Party to this Agreement

Agreement: this contract;

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

Processor Personnel: means all directors, officers, employees, agents, consultants and contractors of the processor and/or of any sub-processor engaged in the performance of its obligations under this Agreement.

GDPR CLAUSE DEFINITIONS:
Data Protection Legislation: (i) all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (ii) (to the extent that it may be applicable) the EU GDPR). The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018.

Data Protection Impact Assessment: an assessment by the Controller carried out in accordance with Section 3 of the UK GDPR and sections 64 and 65 of the DPA 2018.

Controller, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** take the meaning given in the UK GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

UK GDPR: the UK General Data Protection Regulation

Joint Controllers: takes the meaning given in Article 26 of the UK GDPR

Law Enforcement Processing: processing under Part 3 of the DPA 2018.

Protective Measures: appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Agreement, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (Security).

Sub-processor: any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. DATA PROTECTION

1.1. The Parties acknowledge that for the purposes of Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Schedule [X] by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR.

1.2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe Data Protection Legislation.

1.3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

a) a systematic description of the envisaged processing operations and the purpose of the processing;

b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

c) an assessment of the risks to the rights and freedoms of Data Subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

a) process that Personal Data only in accordance with Schedule [X], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

i. nature of the data to be protected;

ii. harm that might result from a Data Loss Event;

iii. state of technological development; and

iv. cost of implementing any measures;

c) ensure that :

i. the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);

ii. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

A. are aware of and comply with the Processor's duties under this clause;

B. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

C. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

D. have undergone adequate training in the use, care, protection and handling of Personal Data; and

d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

i. the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;

ii. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;

iii. the Data Subject has enforceable rights and effective legal remedies;

iv. the Processor complies with its obligations under Data Protection Legislation by providing an appropriate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

v. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the controller on termination of the agreement unless the processor is required by law to retain the personal data.

1.5. Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

a) receives a Data Subject Request (or purported Data Subject Request);

b) receives a request to rectify, block or erase any Personal Data;

c) receives any other request, complaint or communication relating to either Party's obligations under Data Protection Legislation;

d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

f) becomes aware of a Data Loss Event.

1.6. The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller, as details become available.

1.7. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

a) the Controller with full details and copies of the complaint, communication or request;

b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation;

c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

d) assistance as requested by the Controller following any Data Loss Event;

e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

1.8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

a) the Controller determines that the processing is not occasional;

b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10. Each Party shall designate its own data protection officer if required by Data Protection Legislation.

1.11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

a) notify the Controller in writing of the intended Sub-processor and processing;

b) obtain the written consent of the Controller;

c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and

d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 working days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Annex A Part 2: Schedule of Processing, Personal Data and Data Subjects (Schedule X)

Schedule [X] Processing, Personal Data and Data Subjects

This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]
2. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1. [**Guidance:** You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example, where the Parties are Joint Controllers. You should take advice before doing so.]
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide [insert description of relevant service].]
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation 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 or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
International transfers and legal gateway	[Explain where geographically personal data may be stored or accessed from. Explain the legal gateway you are relying on to export the data e.g. adequacy decision, EU SCCs, UK IDTA. Annex any SCCs or IDTA to this contract]
Plan for return and destruction of the data once the processing is complete	[Describe how long the data will be retained for, how it be returned or destroyed]

Annex B: Security

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data. More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR.

The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a supplier) will be held to account to deliver under contract. Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

Examples:

External Certifications: Buyers should ensure that Suppliers hold at least Cyber Essentials Plus certification and ISO 27001:2013 certification if proportionate to the service being procured.

Risk assessment: e.g. The Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

Security classification of information: e.g. If the provision of the services requires the Supplier to Process Authority/Buyer Data which is classified as OFFICIAL,OFFICIAL-SENSITIVE or Personal Data, the Supplier shall implement such additional measures as agreed with the Authority/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

End User Devices e.g.

- The Supplier shall ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority/Buyer except where the Authority/Buyer has given its prior written consent to an alternative arrangement.

- The Supplier shall ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

Testing e.g. The Supplier shall at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.

Networking e.g. The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

Personnel Security e.g. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier may be required to implement additional security vetting for some roles.

Identity, Authentication and Access Control e.g. The supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The supplier must retain records of access to the physical sites and to the service.

Data Destruction/Deletion e.g. The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on.

Audit and Protective Monitoring e.g. The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.

Location of Authority/Buyer Data e.g. The Supplier shall not, and shall procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

Vulnerabilities and Corrective Action e.g. Suppliers shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

Secure Architecture e.g. Suppliers should design the service in accordance with:

- NCSC Security Design Principles for Digital Services
- NCSC Bulk Data Principles
- NSCS Cloud Security Principles