Crown Commercial Service

Procurement Policy Note – Changes to Data Protection Legislation & General Data Protection Regulation

Action Note PPN 02/18 May 2018

Issue

1. New data protection legislation is due to come into force during 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data. Established key principles of data privacy remain relevant in the new data protection legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers.

2. The Data Protection Legislation comprises: i) the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018; and ii) the Data Protection Act (DPA) 2018[1]; and iii) the Law Enforcement Directive.

3. This PPN updates and replaces PPN 03/17. It contains enhanced guidance and clarifications on a number of key areas:

- Controllers and Processors
- Contract Liabilities
- Joint Controllers
- Crown to Crown Data Agreements
- Expired/ Legacy contracts
- Protective Measures
- Enhancements to the standard generic clauses in Annex A:
    - Terminology amendments throughout so that the clause states the "Controller" and "Processor" rather than "Customer" and "Contractor". There is no legal consequence of this change but it will enable the identity of the Controller to be easily varied in Schedule [X] where this is necessary in rare cases.
    - Includes a placeholder for a Joint Controller Agreement at Schedule [Y] where the Parties are Joint Controllers of some of the data under a contract, and clarifies

[1] The Data Protection Bill is currently passing through the House of Commons. Any material changes to the Bill will be reflected in an updated version this PPN.

that the standard clauses will not apply in these instances. Guidance is provided on what is required to be included instead.
    - The term “Data Subject Access Request” has been amended to “Data Subject Request” throughout, so as to clarify that the definition points to any request by a data subject, and not just access requests. There is no legal consequence of this change, this is presentational only.
    - Clause 1.4(b) has been amended so that the Controller is not obliged to approve the “Protective Measures” of the Supplier. Instead, the clause sets out that the Controller may reasonably reject them (although failure to reject shall not amount to approval of their sufficiency by the Controller). This is following concerns raised as to (a) the resources available to check the sufficiency of Protective Measures each time; and (b) the risk that a Processor might argue that the Controller’s approval of inadequate protective measures would excuse the Controller of its failure to provide effective measures.
- Updates in Annex B:
    - Model selection stage questions at 2.6.
    - Model award-stage question at 2.11.
- A new Annex D on technical security considerations.

Dissemination and Scope

4. The contents of this Procurement Policy Note (PPN) apply to all Central Government Departments, their Executive Agencies and Non Departmental Public Bodies. Together these are referred to in this PPN as ‘In-Scope Organisations’. Other public bodies will also be subject to the new data protection legislation and may wish to apply the approaches set out in this PPN.

5. 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.

Timing

6. In-Scope Organisations should already be working towards GDPR compliance for their existing commercial agreements as set out in PPN 03/17, to be compliant by 25 May 2018. This PPN enhances and builds on the content of PPN 03/17, so any contract amendments made using PPN 03/17 are valid. However, for any contract amendments yet to be agreed and for new contracts to be let after 25 May, you should use the provisions of this PPN including the updated standard generic clauses at Annex A. For contracts that concern law enforcement processing, amendments should take effect from the date that the Data Protection Bill comes into force.

Action

7. In line with PPN 03/17 in-Scope Organisations should already have identified existing contracts involving processing personal data which will be in place after 25 May 2018[2] (organisations should have a GDPR implementation lead who will have been compiling this information), and then:

- written to all suppliers notifying them of changes you intend to make to relevant contracts to bring them into line with the new data protection regulations (the draft letter at Annex C provides a guide).
- conducted due diligence on existing contracts to ensure suppliers can implement the appropriate technical and organisational measures to comply with GDPR (i.e. provide guarantees of their ability to comply with the regulations).
- updated the specification and service delivery schedules (the table at Annex A Part 2 provides a guide) to set out clearly the roles and responsibilities of the Controller and the Processor and any Sub-processors.
- updated relevant contract terms and conditions by issuing contract variations, using the change control procedure as set out in your own documentation (the standard generic clauses at Annex A provides a guide).

8. For contracts to be awarded on or after 25 May 2018, In-Scope Organisations should ensure:

- they undertake sufficient due diligence of new Processors to ensure they can implement the appropriate technical and organisational measures to comply with GDPR (i.e. provide guarantees of their ability to comply with the regulations).
- terms and conditions are updated to reflect the standard generic clauses at Annex A,
- for relevant contracts including data processing activities, apply the guidance at Annex B to all stages of the procurement, and relevant documentation.

Key Considerations

Controllers and Processors

9. The GDPR applies to 'Controllers' and 'Processors'. These definitions are broadly the same as under the Data Protection Act 1998 i.e. the Controller says how and why personal data is processed and the Processor acts on the Controller's behalf. Contracts currently subject to the DPA 1998 will likely also to be subject to the GDPR.

- a ***Controller*** is a natural or legal person or organisation which determines the purposes and means of processing personal data; and
- a ***Processor*** is a natural or legal person or organisation which processes personal data on behalf of a Controller.

[2] For law enforcement contracts, this should be from when the Data Protection Bill comes into force.

10. In most cases in public sector contracts, the Controller will be the public body letting the contract or calling-off from the Framework Agreement, and the Processor will be the supplier, but this will not always be the case. Schedule X in Annex A sets out the most common relationship scenarios so that they are agreed within the contract terms. In-Scope Organisations need to identify and agree who is processing the personal data within each contract, and who is determining how, when and where the personal data will be processed (i.e. the Controller).

11. 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.

12. 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. In a contract to deliver pensions administration services, the service could not be delivered without data processing, but the contract may not explicitly mention data processing. 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. In contrast, if the Processor did have an interest in the data for its own purposes, for example for its own marketing purposes outside of the scope of the Controller's instruction, then it would be a Controller in relation to that processing. 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.

13. Further information and guidance is available from the Information Commissioner's Office (ICO) website under the 'Who determines the "purpose and manner" of processing?' section.

Cost of Compliance

14. Any organisation required to comply with the new Data Protection Legislation may incur costs in doing so, especially where new systems or processes are required. However, these costs are attributable to conducting business in the EU, and not supplying the UK public sector. 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

15. In-Scope Organisations found not to be compliant with GDPR by 25 May 2018 will be in breach of the regulations and at risk of being fined, or having an enforcement order issued, by the ICO. The maximum fines available under GDPR are 4% of global annual turnover (for

undertakings) or EUR 20m (for organisations that are not undertakings). An 'undertaking' is any entity engaged in an economic activity offering goods or services in a given market, regardless of its legal status and the way in which it is financed. It does not have to have any intention to earn profits, nor are public bodies excluded. The ICO will take into account the degree of responsibility and other factors.

16. Under the GDPR, Processors now face direct legal obligations (under the current regime this falls solely on Controllers), and they can be fined by the ICO. Both Controllers and Processors can face claims for compensation where they have not complied with their obligations under GDPR.

Contract Liabilities

17. In-Scope Organisations should not accept liability clauses where Processors are indemnified against fines or claims under 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.

18. As the 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. The maximum regulatory fines are set out in paragraph 15; in addition to these fines, the increased rights of data subjects under the 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.

19. 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 €20 million cap on liability for regulatory fines arising out of data protection breach

20. 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.

Joint Controllers

21. There may be instances where In-Scope Organisations are acting as a Joint Controller with another organisation. In these cases, Article 26 of the GDPR states that Joint Controllers must have a transparent 'arrangement' between them which must 'duly reflect the respective roles and relationships of the Joint Controllers vis-à-vis the data subjects'. This need not be a binding contract (as is required by Article 28 in relation to controller-processor relationships) as each joint controller is individually liable for legal compliance under Article 82. The arrangement must clearly set out the roles and responsibilities of each Joint Controller, the relationship each has with the data subjects, and set out the way in which this information will be made available to the data subjects. The arrangement could include, for example, which aspects each Controller will lead on, or be responsible for, to ensure compliance with the GDPR's breach notification obligations.

Crown to Crown Data Agreements

22. Under Section 202 of the current draft of the Data Protection Bill, where a provision of the GDPR or the Act requires relations between a Controller and Processor to be governed by a contract (or other binding legal act) in writing, Crown bodies should use a Memorandum of Understanding (MoU) to satisfy this requirement, on the basis the Crown cannot contract with itself. Crown Bodies should replicate the clauses at Annex A in their MoU to achieve this. A model MoU will be published in due course by DCMS.

Data Processing Outside the UK

23. The GDPR applies to data processing carried out by organisations operating within the EU, including any data processing by those organisations that happens outside the EU. It also applies to organisations outside the EU offering goods or services to individuals in the EU.[3]

Expired/ Legacy Contracts

24. 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 after 25 May 2018 will become subject to the GDPR and this means the Controller must decide whether the data must be retained or deleted.

25. If the Controller decides the data should be deleted, on the basis there is no legal or technical justification to hold it, the Processor should be instructed by the Controller to do so. A Processor continuing to process the data, against the instructions of the Controller, or without the permission of the Controller or without any lawful basis to do so, will be in breach of the GDPR.

26. In instances where personal data needs to be retained by an organisation (whether they are a Controller or Processor), Article 28 of the GDPR will apply to that data from 25 May 2018

[3] Once adopted, the GDPR will also need to be incorporated into the European Economic Area to apply also to EEA countries.

and contract provisions concerning that data must be put in place. 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 since the existing contract will have already expired.

Protective Measures

27. As set out in Article 28(3)(c) 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. There is scope in the future under the GDPR, for approved certification schemes, seals and codes of conduct to demonstrate compliance with the regulations, but these are not yet available and in any event, any one scheme is unlikely to demonstrate full GDPR compliance. Clause 1.13 in Annex A is drafted to allow for the introduction of such schemes.

28. Examples of protective measures might include pre-GDPR information protections under Government contracts such as technical requirements, confidentiality requirements and security provisions. 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 D.

Background

29. Personal data means any information that relates to an identified or identifiable living subject i.e. staff member, member of the public, customer, etc. It will generally include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion, or sexuality. It can also include an individual's email address or job title if that sufficiently picks them out so that they can be identified (in isolation or with other information that may be held). The above is not exhaustive and any information that relates to an individual can be personal data.

30. Information about legal entities such as companies is not personal data, and falls outside the scope of the legislation. Also anonymised or aggregated data is not personal data (unless you also hold the keys to de-anonymise or de-aggregate it.)

31. The definitions are broadly the same as under the Data Protection Act 1998 i.e. the Controller says how and why personal data is processed and the Processor acts on the Controller's behalf. Contracts currently subject to the DPA 1998 will likely also to be subject to the GDPR.

32. The GDPR gives enhanced protection for personal data, and imposes stricter obligations on those who process personal data. The new obligations include:

- When their personal data are collected, individuals must be given more information about how it will be used through enhanced privacy notices.

- Individuals will have much stronger rights to have their personal data rectified, erased and/or provided to them. As a result, the systems used by organisations must be able to honour these rights.

33. For contracts which involve the processing of personal data, In-Scope Organisations must set out, in each contract with suppliers, details of the nature, scope and duration of the data processing, and impose specific obligations on the Processor, including:

i) the legal obligation to formalise working relationships with the Processor in contracts where processing of personal data is to be carried out by a third party on behalf of the Controller (see GDPR Article 28);

ii) a requirement to create and maintain records of processing activities (see GDPR Article 30(2)); and

iii) use only Processors who provide guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will (a) meet the requirements of the GDPR and (b) ensure the protection of the rights of the data subject.

The Law Enforcement Directive (LED)

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

35. Whilst the standard generic clauses at Annex A are compliant with the requirements of Part 3 of the Data Protection Bill, 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

36. The Information Commissioner's Office is a useful source of latest information on GDPR and the LED. DCMS are leading the Data Protection Bill and publish updates on their website here**.** Other sources of information are listed below:-

- ICO Information on GDPR
- General Data Protection Regulations
- ICO information on Data Protection Bill
- Data Protection Bill
- Information Commissioner's guidance on LED
- Law Enforcement Directive

Contact

37. Commercial and procurement enquiries associated with this PPN should be directed to the Crown Commercial Service Helpdesk on 0345 410 2222 or info@crowncommercial.gov.uk.

39. Enquiries on GDPR should be directed to 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 GDPR Clauses

Notes for completion: As the Standard Definitions highlighted below are not specific to GDPR, they should be amended and adapted to fit within your existing contract definitions. The 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

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, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment 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) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** take the meaning given in the 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 the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

Joint Controllers: where two or more Controllers jointly determine the purposes and means of processing

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures: appropriate technical and organisational measures 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 the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule [X]. 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.

1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the 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 (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken 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 EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate 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

(iv) 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 the 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 in phases, 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 by 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 the 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 GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the 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 the 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 Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on 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.

1.15 Where the Parties include two or more Joint Controllers as identified in Schedule [X] in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.

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 Processors, 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 the 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 Controller of some Personal Data: *"Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:* ***[Insert** the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]* *In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."*
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 a service to members of the public.]*
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]*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*

Annex A - Part 3: Schedule for Joint Controller Agreements (Schedule Y)

Schedule Y: Joint Controller Agreement

[Guidance: insert only where Joint Controller applies in Schedule X]

In this Annex the Parties must outline each party's responsibilities for:

- providing information to data subjects under Article 13 and 14 of the GDPR.
- responding to data subject requests under Articles 15-22 of the GDPR
- notifying the Information Commissioner (and data subjects) where necessary about data breaches
- maintaining records of processing under Article 30 of the GDPR
- carrying out any required Data Protection Impact Assessment
- The agreement must include a statement as to who is the point of contact for data subjects.

The essence of this relationship shall be published.

You may wish to incorporate some clauses equivalent to those specified in Clause 1.2-1.14.

You may also wish to include an additional clause apportioning liability between the parties arising out of data protection; of data that is jointly controlled.

Where there is a Joint Control relationship, but no controller to processor relationship under the contract, this completed Schedule Y should be used instead of Clause 1.1-1.15.

Annex B - Guidance for In-Scope Organisations

1) **Existing Contracts continuing after 25 May 2018:**

1.1 In-Scope Organisations should have identified those existing contracts involving processing personal data and which will be in place after 25 May 2018, and then:-

- written to all suppliers notifying them of changes intended to be made to relevant contracts to bring them into line with the new data protection regulations, the draft letter at Annex C provides a guide.
- conducted due diligence on existing contracts to ensure suppliers can implement the appropriate technical and organisational measures to comply with GDPR (i.e. provide guarantees of their ability to comply with the regulations).
- updated the specification and service delivery schedules (the table at Annex A Part 2 provides a guide) to set out clearly the roles and responsibilities of the Controller and the Processor and any sub-processors.
- updated relevant contract terms and conditions by issuing contract variations, using the change control procedure as set out in your own documentation (the standard generic clauses at Annex A provide a guide).

1.2 Organisations who have established Framework Agreements for use by others should have ensured the Framework Terms governing use of the Framework Agreement reflect the standard generic clause at Annex A. They should also have ensured suppliers on the Framework Agreement are aware that Framework Users (i.e. customers) may refine their individual call-offs to assure themselves of compliance with the new data protection legislation.

2) New Contracts due to be let on or after 25 May 2018:

Pre-procurement

2.1 Highlight in any pre-procurement dialogue with potential suppliers that the contract will be subject to new Data Protection Legislation and ensure bidders are both familiar with the new legislation and of their obligations as the Processor. Guidance from the Information Commissioner's Office (ICO) is available here).

2.2 In certain circumstances, the Controller is required to conduct a Data Protection Impact Assessment ("DPIA") prior to any processing (see Article 35 of the GDPR). This may occur before the contract is entered into, and ideally the DPIA should be conducted as early on in the procurement as possible. In all cases advice should be sought from your Data Protection Officer as to whether a DPIA is required. The ICO should publish guidance making clear when a DPIA is required.

2.3 Start to populate Schedule X in order to set out the nature and means of processing etc. This should be refined throughout the procurement and during contract delivery to ensure it is always up to date.

2.4 Information on consent and privacy notices, and data subject's rights under GDPR is available on the ICO website.

Selection Stage

2.5 In procurements for contracts involving processing personal data to be awarded on or after 25 May 2018, due diligence should be undertaken to ensure suppliers can implement the appropriate technical and organisational measures to comply with GDPR and to ensure the protection of the rights of data subjects. Selection criteria should be used to assess suppliers' human and technical resources to perform the contract to the appropriate standard and suppliers should be asked to provide proof by reference to the technical facilities and measures they have in place.

2.6 The Standard Selection Questionnaire will be updated in due course to include a section on GDPR. An example model selection question could be:

A. *Please confirm that you have in place, or that you will have in place by contract award, the human and technical resources to perform the contract to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects. [Yes/ No]*
B. *Please provide details of the technical facilities and measures (including systems and processes) you have in place, or will have in place by contract award, to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects. Your response should include, but should not be limited to facilities and measures:*
    - *to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
    - *to comply with the rights of data subjects in respect of receiving privacy information, and access, rectification, deletion and portability of personal data;*
    - *to ensure that any consent based processing meets standards of active, informed consent, and that such consents are recorded and auditable;*
    - *to ensure legal safeguards are in place to legitimise transfers of personal data outside the EU (if such transfers will take place);*
    - *to maintain records of personal data processing activities; and*
    - *to regularly test, assess and evaluate the effectiveness of the above measures.*

2.7 When evaluating responses, In-Scope Organisations should consider undertaking due diligence and ensure they are satisfied the bidder can provide protective measures appropriate to the nature and risk of the processing. This should be relevant to the subject matter of the contract, and proportionate.

Designing specifications

2.8 Ensure the roles and responsibilities of the Controller and the Processor are set out clearly throughout contract delivery. The Controller must set out clear written instructions for the Processor on how the personal data should be processed, and these must be adhered to by the Processor using Schedule X as the basis. If the Processor does not follow these written instructions, and determines the processing purpose or means of processing themselves, they

will be in breach of contract, and the Processor may be considered to be a Controller in respect of that processing. A typical specification would cover at least the following:-

- the subject matter of the processing;
- details of the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data being processed;
- the categories of the data subjects;
- the obligations and the rights of the Controller;
- that the Processor acts on the documented instructions of the Controller;
- the requirement for the Processor to delete or return the personal data at the end of the provision of services;
- a requirement for the Processor to implement appropriate technical and organisational measures; and
- a right for the Controller to audit the Processor.

2.9 Written instructions should at least set out that the Processor must: -

- process the personal data only on the documented instructions of the Controller;
- comply with security obligations equivalent to those imposed on the Controller (implementing a level of security for the personal data appropriate to the risk);
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- only appoint Sub-processors with the Controller's prior specific or general written authorisation, and impose the same minimum terms imposed on it on the Sub-processor; and the original Processor will remain liable to the Controller for the Sub-processor's compliance. The Sub-processor must provide sufficient guarantees to implement appropriate technical and organisational measures to demonstrate compliance. In the case of general written authorisation, Processors must inform Controllers of intended changes in their Sub-processor arrangements;
- make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller - and the Processor shall immediately inform the controller if, in its opinion, an instruction infringes GDPR or other EU or member state data protection provisions;
- assist the Controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under chapter III of the GDPR, noting different rights may apply depending on the specific legal basis for the processing activity (and should be clarified by the Controller up-front);
- assist the Controller in ensuring compliance with the obligations to implementing a level of security for the personal data appropriate to the risk, taking into account the nature of processing and the information available to the Processor;

- assist the Controller in ensuring compliance with the obligations to carry out Data Protection Impact Assessments, taking into account the nature of processing and the information available to the Processor; and
- notify the Controller without undue delay after becoming aware of a personal data breach.

Procurement Documentation

2.10 Ensure all relevant procurement documents make reference to new Data Protection Legislation coming into force, particularly the details set out in Schedule X agreed pre-procurement, and update terms and conditions using the generic standard clause at Annex A as the basis. Seek legal advice to ensure this fits the nature of the requirement and the other documentation used. A DPIA may be undertaken after contract award but prior to any processing with support from the Processor, factoring in time to consult the ICO if the DPIA relates to high risk processing.

Award Stage

2.11 For procurements involving personal data processing, and particularly those for high risk processing, In-scope Organisations should ensure bidders are asked, at award stage, how the technical and organisational measures put in place (and set out at selection stage) meet the needs of the contract. For example, a model award question to ask bidders might be:-

Please provide details of the key data protection risks you foresee with this Contract and set out your proposals for dealing with those risks

Contract Management / Supplier Assurance

2.12 Build into contract management activities sufficient checks to ensure suppliers are meeting their obligations under the new Data Protection Legislation as the Processor. These supplier assurance activities may include audits undertaken by the Controller or a third party auditor. If obligations are not being met, take urgent remedial action with the supplier to address issues and risks.

Using Framework Agreements

2.13 When using Framework Agreements, including those established by Crown Commercial Service (CCS), Customers should review each call-off to ensure roles and responsibilities have been updated to reflect Data Protection requirements. For CCS agreements, a customer toolkit has been developed to provide guidance on the actions customers need to take on call-off contracts to comply with GDPR.

2.14 Where contracts are formed on the basis of a supplier's terms and conditions, such as when using the CCS G-Cloud framework, supplier's terms must not prevail. This should be set-out in the Framework documentation, but In-Scope Organisations should check to ensure they are satisfied this is sufficient and supplement where necessary.

3) Contractual arrangements relying solely on the supplier's terms and conditions

3.1 Where you are relying solely on a supplier's terms and conditions, you must ensure that these meet the requirements of the data protection legislation.

3.2 This is most likely to arise in the use of IT services into which personal data (such as names, email addresses, etc) are placed, and where the supplier is acting as a Processor. There are many examples of cloud-based services that handle personal data, and where standard terms and conditions are generally relied upon. If these services are used to hold personal data, then the terms and conditions must reflect the content of the standard draft generic clauses at Annex A. In these cases the onus is on the service supplier to ensure that their terms and conditions are legally compliant, but In-Scope Organisations have an obligation not to use services that are not compliant.

3.3. Some IT service suppliers use "data processing agreements" that sit alongside their terms and conditions and supplement them in order to satisfy data protection law. These data processing agreements may need to be actively signed and returned to the supplier before they are legally binding. If you are unsure, consult your Data Protection Officer.

Annex C – Draft Letter for Suppliers

[Insert draft text, amending as appropriate]

New data protection legislation is due to come into force during May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data.

Established key principles of data privacy will remain relevant in the new Data Protection Legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers. The new General Data Protection Regulations specify that any processing of personal data, by a Processor, should be governed by a contract with certain provisions included.

We have identified a number of existing contracts involving processing personal data, and which will be in place after 25 May 2018, that require updating to bring them into line with the new regulations and these are listed below. This will involve updating contract terms based on the generic standard clauses published in Procurement Policy Note 03/17 and ensuring specifications and service delivery schedules reflect the roles and responsibilities between the Controller and the Processor as required by the new regulations.

[Insert or attach list of relevant contracts]

In addition, we will be updating our procurement documentation to reflect the new regulations for contracts to be awarded on or after 25 May 2018.

Any organisation required to comply with the new Data Protection Legislation may incur costs in doing so, especially where new systems or processes are required. However, these costs are attributable to conducting business in the EU, and not supplying the UK public sector. We expect all suppliers to manage their own costs in relation to compliance.

As the Controller, we will not accept liability clauses where you are indemnified against fines under GDPR as the Processor. The legal penalty regime has been extended directly to Processors to ensure better performance and enhanced protection for personal data. That means indemnifying Processors for any GDPR fines or court claims undermines these principles.

Our Commercial Teams will contact you in the coming weeks to start work on varying existing contracts. You may also have received similar communications from commercial teams across the public sector.

If you would like to know more about the upcoming changes, the Information Commissioner's Office is a useful source of information on the new regulations (ICO Information on GDPR).

Annex D: 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 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.

External Certifications e.g. 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. 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 maybe 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"