Crown Commercial Service

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

Action Note PPN 03/17 December 2017

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 which is anticipated to come into force (subject to Parliamentary approval[1]) on 6 May 2018 for law enforcement processing, and 25 May for GDPR.

Dissemination and Scope:

3. 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.

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.

[1] The Data Protection Bill is currently undergoing committee scrutiny in the House of Lords. Any material changes to the Bill will be reflected in an updated version this PPN.

Timing:

5. In-Scope Organisations must begin to apply the provisions of this PPN immediately, ensuring any contract amendments take effect from 25 May 2018 and new provisions are applied to all new relevant contracts awarded on or after 25 May 2018. For contracts that concern law enforcement processing, amendments should take effect from 6 May 2018.

Action:

6. In-Scope Organisations should identify existing contracts involving processing personal data which will be in place after 25 May 2018[2] (most organisations should already have a GDPR implementation lead who will have been compiling this information), and then:

- write 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).
- conduct 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).
- update 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.
- update 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).

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

- they undertake sufficient due diligence of new suppliers 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

8. 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

[2] For law enforcement contracts, this should by 6 May 2018

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.

9. 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. However, In-scope Organisations should check who determines the purposes and means of processing personal data before they establish themselves as the Controller.

Cost of Compliance

10. 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 with new Data Protection Legislation.

Risks of Non-Compliance

11. In-Scope Organisations found not to be GDPR compliant 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 Information Commissioner's Office (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.

12. 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

13. 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 GDPR fines or court claims undermines these principles.

Joint Controllers

14. 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 have to 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'.

Data Processing Outside the UK

15. 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]

Background:

16. 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.

17. 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.)

18. 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.

19. 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.

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

20. 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)

21. 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.

22. 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:

23. 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:

23. 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.

24. 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 Contractor is bound to comply;

Contractor Personnel: means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor 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 Contractor 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 Access 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)*

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.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Contractor 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. The only processing that the Contractor is authorised to do is listed in Schedule [X] by the Customer and may not be determined by the Contractor.

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

1.3 The Contractor shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, 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 Contractor 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 Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event 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 Contractor 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 Contractor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Contractor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Contractor 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 Customer 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 Customer has been obtained and the following conditions are fulfilled:

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

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

(iii) the Contractor 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 Customer in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Contractor shall notify the Customer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access 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 Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide the Customer 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 Customer) including by promptly providing:

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

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

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

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

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

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

(a) the Customer determines that the processing is not occasional;

(b) the Customer 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; and

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

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

1.10 The Contractor shall designate a 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 Contractor must:

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

(b) obtain the written consent of the Customer;

(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 Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Customer 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 Customer may on not less than 30 Working Days' notice to the Contractor 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] Processing, Personal Data and Data Subjects

1. The Contractor shall comply with any further written instructions with respect to processing by the Customer.

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
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	*[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 B - Guidance for In-Scope Organisations

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

1.1 In-Scope Organisations should ensure they have identified those existing contracts involving processing personal data and which will be in place after 25 May 2018. The key actions required are as follows:-

- write 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.
- conduct 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).
- update the specification and service delivery schedules (the table at Annex A Part 2 as provides a guide) to set out clearly the roles and responsibilities of the Controller and the Processor and any sub-processors.
- update 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 ensure the Framework Terms governing use of the Framework Agreement reflect the standard generic clause at Annex A. They should also ensure 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 Information on consent and privacy notices. and data subject's rights under GDPR is available on the ICO website.

Designing specifications

2.4 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. If the Processor does not follow these written instructions, and determines the processing purpose or means of processing themselves, the Processor will 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.

2.5 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

2.6 Ensure all relevant procurement documents make reference to new Data Protection Legislation coming into force, 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.

Contract Management / Supplier Assurance

2.7 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

2.8 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.

2.9 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).