

Appendix 2 - Data protection compliance template

Appendix 2

Data Protection Act Compliance Check Template

This checklist aims to assist organisations proposing change to investigate whether the personal information aspects of their project comply with the Principles in Schedule 1 of the Data Protection Act (DPA).

It has been designed as a template to be deployed on desktops, portable computers (provided they are secure) or internal websites for use by any employee proposing change. Where so adopted by agencies, the template may need to be modified to add organisation-specific details.

It should be noted that many terms used in the [Schedule 1 Principles](#) have meanings specific to the [Data Protection Act](#), and it would be prudent to refer to the Act for definition for those terms. Another useful reference in this regard is the [Information Commissioner's Legal Guidance](#). Users are also encouraged to seek guidance from sources such as the organisation's Data Protection Officer, legal unit or external lawyers/ consultants.

BASIC INFORMATION – New Project

1. Organisation and Project

Organisation	DCUSA Ltd
Branch / Division	Governance Services
Project	Theft of Electricity Code of Practice

2. Contact Position and/or Name, Telephone Number and Email Address.

Name, Title	
Branch / Division	Governance Services – DCUSA Ltd
Phone Number	
E-Mail	

3. Description of the Program / System / Technology / Legislation (Initiative) being assessed.

- A DCUSA Schedule which details both obligations and best practice for Parties (Suppliers and Distributors) in detecting, investigating, resolving and preventing abstraction of electricity. Parties must ensure that where they use agents to discharge their obligations they shall adhere to the Theft of Electricity Code of Practice.

4. Purpose / Objectives of the initiative (if statutory, provide citation).

- The CoP outlines the relationships between Parties where abstraction of electricity is suspected and/or confirmed. It sets out a number of obligations and minimum service standards that Parties are expected to meet in relation to:
 - Communication between Parties where abstraction of electricity is suspected or confirmed;
 - Procedures for investigation where abstraction of electricity is suspected or confirmed;
 - Procedures for site visits and gaining entry to premises where abstraction of electricity is suspected or confirmed;
 - The manner in which Parties will deal with Consumers who are suspected of and are identified as having taken electricity illegally (defined in this document as “abstraction of electricity”);
 - The manner in which Parties will treat Vulnerable Customers where Abstraction of electricity is suspected or confirmed;
 - The manner in which unrecorded units are to be assessed;
 - De- energisation and Disconnection of Supply where abstraction of electricity is suspected or confirmed; and

- Provision of information following investigation where Abstraction of electricity is suspected or confirmed

5. What are the potential privacy impacts of this proposal?

- Personal data being shared between the Parties;
- Passing of factual information registered against an individual between parties.
- Passing of unproven facts, registered against an individual, between Parties;
- Passing information to external Parties such as care agents, social services etc as well as their ability to maintain confidentiality;
- Sharing information with a Consumer's representative.

6. Provide details of any previous PIA or other form of personal data* assessment done on this initiative (in whole or in part).

- Not applicable

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO III DPA COMPLIANCE – CONCLUSIONS

***IMPORTANT NOTE:**

'Personal data' means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

(Data Protection Act, section 1)

II DATA PROTECTION PRINCIPLES (DPPs)

1 Principle 1: Fair and Lawful Processing

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- (a) at least one of the conditions in Schedule 2 is met, and
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 19-35

1.1 Preliminary

1.1.1 What type of personal data are you processing?

- Non-sensitive personal data such as supply information attributed to the premises, at which theft is suspected to have occurred by a Consumer.
- Consumer name
- Site address
- Consumer contact details eg. Telephone numbers; email addresses
- Consumer age
- A list of data items which Parties may utilise to transfer information is set out in the MRA D0238 data flow.

Please give examples of any sensitive personal data that you are processing.

- Vulnerability;

- Details around suspicion of theft;
- Details of confirmed previous offences
- Physical Risk eg. Customer behaviour, needle stick injuries

1.1.2 Are sensitive personal data being differentiated from other forms of personal data?

- No

If yes, please specify procedures. If no, please indicate why not.

- Management of all personal data will be treated as sensitive personal data.

1.2 Schedule 2 - Grounds for Legitimate Processing of Any Personal Data

1.2.1 Have you identified all the categories of personal data that you will be processing and how?

- No

If yes, please list them. If no, please indicate why not.

- Because all personal data is being treated as sensitive personal data.

1.2.2 Have you identified the purposes for which you will be processing personal data and how?

- Yes

If yes, please list them. If no, please indicate why not.

- For the detection and prevention of theft;
- To determine the theft period

- To accurately assess the energy stolen over the theft period;
- To ensure Parties meet legal and regulatory obligations.
- To protect Vulnerable consumers

1.2.3 Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data?

- Yes

If yes, please list them. If no, please indicate why not.

- The processing is necessary for the performance of a contract to which the data subject to a party;
- The process is necessary for compliance with any legal obligation to which the Data Controller/Processor is subject other than an obligation imposed by a contract;
- The process is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person;
- The process is necessary for the administration of justice; and
- The processing is in accordance with the legitimate interest of the Data Controller/Processor to detect and prevent theft.

1.2.4 Are you relying on different grounds for different categories of personal data?

- No

If yes, how will this assessment be made?

1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data

If this project does not involve the processing of sensitive personal data, please go to section 1.4

1.3.1 Have you identified the categories of sensitive personal data that you will be processing?

- Yes

If yes, can you list them. If no, please indicate why not.

- Vulnerability status – Physical and mental health information; and
- Allegation of committing a criminal offence
- Potential for physical risk to parties agent attending site

1.3.2 Have you identified the purposes for which you will be processing sensitive personal data?

- Yes

If yes, can you list them. If no, please indicate why not.

- For the detection and prevention of theft;
- To accurately assess the energy stolen over the theft period;
- To ensure Parties meet legal and regulatory obligations.

1.3.3 Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data?

- Yes

If yes, can you list them. If no, please indicate why not.

- The processing:
 - is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - is necessary for the purpose of obtaining legal advice,
 - is otherwise necessary for the purposes of establishing, exercising or defending legal rights; or

- Is necessary for the administration of justice

1.3.4 Are you relying on different grounds for different categories of sensitive personal data?

- No

If so, how will this assessment be made?

- Not applicable

1.4 Obtaining consent

1.4.1 Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?

No

If yes, when and how will that consent obtained?

1.4.2 For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act?

- No

If so, when and how will that consent obtained?

1.5 Lawful Processing

a. If you are a public sector organisation: N/A

1.5.1 Does your processing of personal data fall within your statutory powers?

N/A If yes, please state what they will be. If no, please indicate why not.

- N/A

1.5.2 How is compliance with the Human Rights Act being assessed?

- N/A

b. All organisations:

1.5.3 Are you assessing whether any of the personal data being processed is held under a duty of confidentiality?

- Yes

If yes, how will that assessment made? If no, please indicate why not.

- Data will only be shared with organisations which would be expected to have in place appropriate confidentiality policies.
- Data will not be shared with organisations which cannot demonstrate the above.

1.5.4 How is that confidentiality maintained? (eg instructions on disclosure or shredding)

- Confidentiality of data will be maintained through organisations' own data protection policies and procedures.

1.5.5 Are you assessing whether your processing is subject to any other legal or regulatory duties?

Yes

If yes, how is that assessment being made? If no, please indicate why not.

- Against the pending Electricity Supply License conditions and the Electricity Act.
- The sharing of data is required to demonstrate preventative measures under the DCUSA Schedule ?? – Theft of Electricity Code of Practice.

1.5.6 How are you ensuring that those legal duties are being complied with?

- By complying with the abstraction of electricity CoP which is being brought under the DCUSA.
- Parties will ensure legal duties are complied with through their internal compliance assurance procedures and policies.

1.6 Fair Processing

1.6.1 Are individuals being made aware of the identity of your organisation as the data controller?

Yes

If yes, state how they are being made aware. If no, please indicate why not.

- By providing ID on every visit and all correspondence on the matter contains contact details.
- Suppliers will make Customers aware through their Privacy statements within their terms and conditions. All Parties will re-iterate their policies on sharing data at appropriate opportunities in the course of operating under the CoP.

1.6.2 How are individuals being made aware of how their personal data is being used?

- During all verbal and written communication.
- Suppliers will make Customers aware through their Privacy statements within the terms and conditions.

1.6.3 How are individuals offered the opportunity to restrict processing for other purposes?

- Not applicable under the scope of this exercise.

When is that opportunity offered?

- N/A

1.6.4 Do you receive information about individuals from third parties?

- Yes

If yes, please give examples. If no, please go to section 1.7

- Information about individuals may be received from:-
 - Market participants
 - Members of the public e.g neighbours; anonymous tip-offs
 - Public bodies such as , Police, Local Authority social services, Consumer Focus, UKRPA,

1.6.5 How are individuals informed that the data controller is holding personal data about them?

- The occupier of the property will be in contract with the Supplier whether deemed or explicit and therefore will have consented to personal data being held.
- During every visit; all correspondence on the matter contains contact details.

When are individuals informed?

- During every visit – either on arrival or when leaving the site, or as soon as possible thereafter.

1.7 Exemptions from the First Data Protection Principle

The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:-

1. the identity of the data controller
2. the identify of any nominated data protection representative, where one has been appointed
3. the purpose(s) for which the data are intended to be processed
4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Data Protection Act, Schedule 1, Part II, para. 2 (3)

1.7.1 Do you provide individuals with all of the information in the box above?

- Yes – believed to be covered via individual Supply License conditions, the National Terms of Connection and the Electricity [Act](#)

If no, which exemption to these provisions is being relied upon?

2 Principle 2: Purpose Limitation

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

For the Information Commissioner's guidance in relation to this DPP, see [Legal Guidance](#) pp 35-6

2.1 Uses of Personal Data within the Organisation

2.1.1 Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?

- Yes

2.1.2 How often is this record checked?

- Frequency of updating records is carried out in accordance with individual organisations' data privacy policies

2.1.3 Does the record cover processing carried out on your behalf (eg by a subcontractor)?

- This will be managed within each organisation

2.1.4 What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data?

(Cross reference with section 1.6, Fair Processing)

- Parties shall be informing Customers through written and verbal communication as detailed in the Code of Practice.

2.2 Use of Existing Personal Data for New Purposes

2.2.1 Does the project involve the use of existing personal data for new purposes?

- Yes – specifically passing information between PartiesThe use of existing personal data for the prevention of fraud has already been anticipated and covered off in many companies' terms and conditions.

If no, go to section 2.3

2.2.2 How is the use of existing personal data for new purposes being communicated to:-

(a) the data subject;

- Through existing terms and conditions

(b) the person responsible for Notification within the organisation

- Representatives of any Parties subject to the CoP shall inform their respective members of staff responsible for the notification.

(c) the Information Commissioner?

- Members of the Theft of Electricity CoP working group as well as representatives within individual companies have liaised on several occasions with the ICO to ensure the Theft/Abstrcation of Electricity CoP complies with the provisions as set out in the DPA.

2.2.3 What checks are being made to ensure that further processing is not incompatible with its original purpose?

- Parties will carry out internal audits to ensure the DPA is being adhered to.

2.3 Disclosures of Data

2.3.1 Do you have a policy on disclosures of personal data within your organisation / to third parties?

- Yes Individual companies need to ensure they adhere to DPA

Is it documented?

- Yes Individual companies are responsible for this.

2.3.2 How are staff made aware of this policy / instructed to make disclosures?

- Individual organisations are responsible for making its staff aware of the relevant policies on the disclosure of personal data within their organisation to third parties.

2.3.3 How are individuals / data subjects made aware of disclosures of their personal data?

- Managed by individual companies.

2.3.4 Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed?

- Yes

If no, go to section 3.1

If yes, how do you make the assessment?

- Individual organisations are responsible for assessing the compatibility of a 3rd party's use of the personal data to be disclosed.

3 Principle 3: Adequate, Relevant and Not Excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For the Information Commissioner's guidance in relation to this DPP, see [Legal Guidance](#) pp 36-37

3.1 Adequacy and relevance of Personal Data

3.1.1 How is the adequacy of personal data for each purpose determined? (Please give examples.)

- Data, relating to both suspected and confirmed theft cases, is being passed on by the Supplier to the new Supplier on a change of Supplier, to welfare organisations and to 3rd parties where necessary;
- Sharing vulnerability status, meter status, consumer behavior and reason for disconnection with care agencies;
- Non-routine exchange of data between existing and previous Supplier.

3.1.2 How is an assessment made as to the relevance (ie no more than the minimum required) of personal data for the purpose for which it is collected?

- Only information necessary to the investigation in accordance with agreed procedures between Parties is exchanged.

3.1.3 What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?

- The CoP sets out what is adequate, relevant and not excessive.

How often will these procedures reviewed?

- The CoP falls under DCUSA governance.

3.1.4 Are there procedures for assessing the amount and type of personal data collected for a particular purpose?

- Yes.

If yes, please describe. If no, please indicate why not.

The CoP sets out the procedures.

3.1.5 Are items of personal data held in every case which are only relevant to a subset of those cases?

- Yes

4 Principle 4: Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date.

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 37-8

4.1 Accuracy of Personal Data

4.1.1 Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?

- Yes

4.1.2 How, and how often, are personal data be checked for accuracy?

Please give examples:

- Data shared between Parties may be a mixture of evidence or suspicion;
- Data shared between Parties and care agencies would be fact-based.

4.1.3 In what circumstances is the accuracy of the personal data being checked with the Data Subject?

Please give examples:

- During the course of each Abstraction of electricity investigation;
- The Vulnerability status would be verified with the Consumers or their nominated spokesmen.

4.1.4 Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record?

- Yes

If so, how? Please give examples:

- Parties and their agents will endeavour to collect evidence and information of a standard to substantiate court proceedings (whether criminal or civil, according to Parties' policies), using rules for collection and safe keeping of evidence.

4.1.5 Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate?

- Yes – as part of any investigation

If no, please indicate why not.

4.2 Keeping Personal Data Up to Date

4.2.1 Are there procedures to determine when and how often personal data requires updating?

- Yes

4.2.2 Are personal data evaluated to establish the degree of damage to:

(a) the data subject

or

(b) the data controller

that could be caused through being out of date?

- Parties acknowledge there are risks associated to both the data subject and the data controller if out of date personal data is shared.

Please specify whether to data subject or data controller:

4.2.3 Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?

- No – wherever possible the use of free text should be avoided and only facts and no opinions should be shared.

5 Principle 5: No Longer than Necessary

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance p 39

5.1 Retention Policy

5.1.1 What are the criteria for determining retention periods of personal data?

- Parties should ensure consumer data relevant to the investigation is retained no longer than reasonable required.

How often are these criteria reviewed?

- In line with any changes to the Data Protection Act

5.1.2 Does the project(s) include the facility to set retention periods?

- No

5.1.3 Is the project subject to any statutory / sectoral requirements on retention?

- Yes

If yes, please state relevant requirements:

- Retention of exhibits – statutory limitations to retain all tampered meters for a minimum of 6 months and any physical evidence required for prosecution for a minimum of 12 months.
- Retention of documentary and supporting evidence for a period of 6 years.

5.2 Review and Deletion of Personal Data

5.2.1 Is there a review policy?

- Yes

Is it documented?

- Yes

5.2.2 When data is no longer necessary for the purposes for which it was collected:

(a) How is a review made to determine whether the data should be deleted?

- In line with individual organisations' retention policy

(b) How often is the review be conducted?

- In line with individual organisations' retention policy

(c) Who is responsible for determining the review?

- Individual organisations privacy teams.

(d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?

Yes No

- This will be determined by individual organisations DPA Policy.

5.2.3 Are there any exceptional circumstances for retaining certain data for longer than the normal period?

- Yes

If yes, please give justification:

To be determined by individual organisations.

5.2.4 Is there any guidance on deletion / destruction of personal data?

Yes If no, please indicate why not.

6 Principle 6: Data subject access

Personal data shall be processed in accordance with the rights of data subjects under this Act.

For the Information Commissioner's guidance in relation to this DPP, see [Legal Guidance](#) pp 39-40

6.1 Subject Access

6.1.1 Are procedures in place to provide access to records under this Principle?

- Yes

If yes, please specify proposed procedures. If no, please indicate why not.

- Covered by current Data Protection Act practices

6.1.2 How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?

- Covered by current Data Protection Act practices

6.1.3 Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject?

- Yes

If yes, how? If no, please indicate why not.

- Covered by current Data Protection Act practices

6.1.4 Are procedures in place to manage personal data relating to third parties?

- Yes

If yes, please specify proposed procedures. If no, please indicate why not.

- Covered by current Data Protection Act practices

6.1.5 How is data relating to third parties managed?

- Covered by current Data Protection Act practices

6.2 Withholding of personal data in response to a subject access request

6.2.1 Are there any circumstances where you would withhold personal data from a subject access request?

Yes

If no, go to section 6.3. If yes, on what grounds?

- Circumstances where personal data is withheld from a subject access request is the responsibility of individual companies.

6.2.2 How are the grounds for doing so identified?

- In accordance with individual companies procedure

6.3 Processing that may cause Damage or Distress

6.3.1 Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?

- Yes

If yes, please specify proposed procedures. If no, please indicate why not.

- Organisations individually assess how to avoid causing unwarranted or substantial damage or distress to an individual.

6.3.2 Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?

- Yes

6.4 Right to Object

6.4.1 Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?

- Not applicable

6.5 Automated Decision-Taking

6.5.1 Are any decisions affecting individuals made solely on processing by automatic means?

- Not applicable

If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?

6.6 Rectification, Blocking, Erasure and Destruction

6.6.1 What is the procedure for responding data subject's notice (in respect of accessible records) or a court order requiring:

- (a) rectification;
- (b) blocking;
- (c) erasure or;
- (d) destruction of personal data?

- **Procedure for responding to a data subject's notice (in respect of accessible records or a court order requiring rectification, blocking, erasure or destruction of personal data is managed by individual organisations.**

7 Principle 7: Data Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 40-3

7.1 Security Policy

7.1.1 Is there a Data Security Policy?

Yes

If no, please indicate why not and then go to 7.1, question 5..

7.1.2 If yes, who / which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?

- Individual Parties are responsible for drafting and enforcing the Data Security Policy within the organisation.

7.1.3 Does the Data Security Policy specifically address data protection issues?

Yes

7.1.4 What are the procedures for monitoring compliance with the Data Security Policy within the organisation?

- These will be managed by the Individual Organisations.

7.1.5 Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?

Yes

7.1.6 Is the level of security appropriate for the type of personal data processed?

Yes

7.1.7 How does the level of security compare to industry standards, if any?

Data is expected to be exchanged via a secure network. Any additional information requested direct between parties will be sent by encrypted e-mails.

7.2 Unauthorised or unlawful processing of data

7.2.1 Describe security measures that are in place to prevent any unauthorised or unlawful processing of:

(a) Data held in an automated format (eg password controlled access to PCs)

(b) Data held in a manual record (eg locked filing cabinets)?

- Security measures to prevent any unauthorised or unlawful processing are managed by individual organisations.

7.2.2 Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing?

Yes

If yes, please describe the planned procedures. If no, please indicate why not.

- Procedures to secure and protect sensitive personal data from unauthorised or unlawful processing are managed by individual organisations.

7.2.3 Describe the procedures in place to detect breaches of security (remote, physical or logical)?

- These are the responsibility of the individual organisations.

7.4 Destruction of Personal Data

Cross-reference with section 5.2

7.4.1 Describe the procedures in place to ensure the destruction of personal data no longer necessary?

- Procedures to ensure the destruction of personal data no longer necessary are managed by individual organisations.

7.4.2 Are there different procedures for destroying sensitive personal data?

This is managed by individual organisations.

7.5 Contingency Planning - Accidental loss, destruction, damage to personal data

7.5.1 Is there a contingency plan to manage the effect(s) of an unforeseen event?

Yes

7.5.2 Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through:

- human error
- computer virus
- network failure
- theft
- fire
- flood
- other disaster.
 - Individual companies have their own risk management procedures to recover data (both automated and manual) which may be damaged or lost

8 Principle 8: Overseas Transfer

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For the Information Commissioner's guidance in relation to this DPP, see [Legal Guidance](#) pp 43-5

8.1 Adequate Levels of Protection

8.1.1 Are you transferring personal data to a country or territory outside of the EEA?

No

If no, please go to Part III.

If yes, where?

8.1.2 What are the types of data are transferred? (eg contact details, employee records)

- N/A

8.1.3 Are sensitive personal data transferred abroad?

- N/A

If yes, please provide details:

8.1.4 What are the main risks involved in the transfer of personal data to countries outside the EEA?

- N/A

8.1.5 Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?

- N/A

8.1.6 Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?

- N/A

8.2 Exempt Transfers

8.2.1 Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply?

Yes No

If yes, what are they?

- N/A

8.2.2 To which country / territory are these transfers made?

- N/A

8.2.3 What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle?

Eg consent, (See DPA 1998, Schedule 4, for a full list)

- N/A

8.3 Choosing a Data Processor

8.3.1 What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?

- N/A

8.3.2 How did you assess their data security measures?

- N/A

8.3.3 How do you ensure that the Data Processor complies with these measures?

- N/A

8.3.4 Is there an on-going procedure for monitoring their data security measures?

N/A If yes, please describe. If no, please indicate why not.

- N/A

III DPP COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

_____ (Proponent) Date: _____

_____ (Data Protection Officer) Date: _____

[« Previous](#) | [Top of page](#) | [Next »](#)