Version 1.0

Appendix F: DPA Checklist for G-Cloud Suppliers

The following is the Checklist for Suppliers of G-Cloud Services and is based on the Information Commissioner's PIA Handbook and Personal Information Online (code of Practice).

Suppliers of G-Cloud services will generally be 'Data Processors' under the Data Protection Act (DPA). The organisations using their services will generally be 'Data Controllers'. Data controllers have the legal duty to comply with the DPA. However, service providers can help them to do this by ensuring that their IA documentation for G-Cloud provides clear evidence of how their service will allow the consuming organisation to complete its Privacy Impact Assessment and in turn to comply with the DPA. **Please note that reference to "Personal Data" in this checklist also includes Sensitive Personal Data (as defined under the DPA).** Therefore, the G-Cloud programme is expecting suppliers demonstrate that their services are appropriate for Sensitive Personal Data.

Please note that the advice of the ICO to consuming organisations is that if the service supplier cannot provide satisfactory answers to any of the questions below, then this should raise concerns about the supplier's ability to look after the information you have entrusted to it. If this is the case, potential consumers should not use the provider concerned and should seek alternatives. Remember that the ultimate responsibility for information remains with the 'data controller'.

ID.	Service supplier checklist	Evidence, including paragraph-level reference to corresponding IA documentation
1.	Can you provide written guarantees about your security arrangements?	
2.	How will you guarantee that you will only process personal data in accordance with your clients' instructions, e.g. How will you maintain an appropriate level of security? Ensure that personal data will not be retained for longer than instructed?	
3.	How will you guarantee that your staff are trained and vetted to suitable standards, wherever they are based?	
4.	What are your complaints and redress procedure,	

	e.g. do you offer compensation for loss or corruption of clients' data?	
5.	Can you ensure that any information identified as 'personal data' within the information provided to you will be protected adequately, e.g. prevent any unauthorised or unlawful processing of personal data within the service? Does your service allow the Data Controller to create and maintain a comprehensive and up to date record of personal data usage? What facilities do you have that would help your client to locate all personal data items falling within a 'subject access request' as defined by the DPA?	
6.	What facilities do you have to comply with your client's instructions on (a.) rectification, (b.) blocking, (c.) erasure, or (d.) destruction of personal data? Note that the instructions to carry out these measures may be placed on the Data Controller by Court Order.	
7.	If information is not erased or destroyed as a result of positive instruction from the consumer (see question (6.)), how long will data is likely to be retained and in which forms)? What are the best and worst cases for when suppliers can give assurance that the information will have been overwritten (include the retention on archive and back up systems).	
8.	How does your service allow the client to change/restrict the use of particular personal data items?	
9.	Does your service offer the ability to flag records for review /deletion? If so how is this achieved?	
10.	How can you help your client to maintain the accuracy of the records at all times (e.g. the Integrity of the information)?	
11.	Can you provide your consumers with copies of their information regularly, in an agreed format and structure, so that they hold useable copies of vital information at all times?	
12.	Can you ensure that your service will continue to maintain high data protection standards, taking in to account the development in security products and	

	the cost of deploying or updating these?	
13.	How do you restrict access to personal data by members of your own staff? What reporting arrangements will you have in place, for example for informing your client of a security breach?	
14.	Can you provide any guarantees as to where personal data will be located geographically? Note that the DPA contains rules about the transfer of personal data outside the EEA. This means that you should be able to tell your clients where any of the personal data they provide to you is located at any particular time. .	
15.	If your service will involve personal data being outside the EEA, what measures are in place to ensure that levels of protection during its transfer, storage and processing are adequate?	
16.	Can you ensure that your service will continue to maintain high data protection standards even if you store data in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?	
17.	Can you guarantee the reliability and training of your staff, wherever they are based? Do they have any form of professional accreditation?	
18.	What capacity does the service have for recovering from a serious technological or procedural failure? E.g. human error, computer virus, network failure, theft, fire, flood, other disasters	
19.	How will you demonstrate ongoing compliance with the assurances you have given?	
20.	How will you report breaches of security and security incidents to your client?	

For information about overseas transfers, see:
http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx

Further guidance is available in The Guide to Data Protection at:
http://www.ico.gov.uk/home/for_organisations/data_protection_guide.aspx

The ICO code of practice on managing personal information online is available at:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online.aspx