Greater London Authority (GLA)

Road User Charging Appeal Service

Appendix 1 –

Information Governance
Statement of Requirements

Table of Contents

1 Privacy Notice

1.1 Introduction

1.1.1 GLA requires the Service Provider to have an appropriate Privacy Notice (also sometimes known as a data protection or fair processing notice) to be made available to Customers when they provide their personal Information. The Notice will be subject to change depending upon policy and regulatory requirements.

1.1.2 The provision of the Privacy Notice forms part of GLA's compliance with the first principle of the Data Protection Act 1998 (DPA).

The following requirements detail the circumstances and method of presentation, but by way of illustration, the Privacy Notice shall be:

- displayed for acknowledgement on the Service's Website before submission of Personal Data;
- provided as a recording on the IVR system;
- provided on Customer's request.
- Displayed on relevant outgoing correspondence and guidance notes, but not Statutory Decision Notices;
- available via the internet.

2 Data Subject Request Processes

2.1 Introduction

The Service Provider shall implement a procedure that shall be agreed with GLA to respond to Subject Access Requests made under section 7 of the Data Protection Act 1998 (DPA), which incorporates the obligation to respond appropriately to requests received from individuals wishing to exercise their rights to:

- prevent processing likely to cause damage or distress,
- prevent direct marketing and
- request a manual assessment of any automated decision taking, currently provided for under sections 10, 11 and 12 of the Data Protection Act respectively.

2.2 Definitions

A 'Data Controller' is a person or organisation that decides the purposes for which personal Information will be used and how it will be processed. The Service Provider is the Data Controller in relation to Personal Data processed in connection with the Appeals Service.

A Data Processor is any person (other than an employee of the Data Controller) who processes Personal Data on behalf of the Data Controller. The Adjudicators are Data Processors in relation to Personal Data processed in connection with the Road User Charging Scheme(s).

A Data Subject means an individual who is the subject of Personal Data.

2.3 What are 'Subject Access Requests'?

Under Section 7 of the DPA any person has the right to contact any 'Data Controller' they believe holds Information about them and request a copy of that Information.

Applicants are also entitled to be told:

- the purposes for which the Information is being used;
- the recipients or types of recipients to whom the Information may be disclosed;
- any available Information as to the sources of the Information;
- an explanation of any codes, abbreviations etc. used; and
- Information about the reasoning behind any decisions taken by automated means.

Subject Access Requests (SARs) must be made in writing and are subject to an administration charge in accordance with Regulation 3 of the Data Protection (Subject Access)(Fees and Miscellaneous Provisions) Regulations 2000. Currently the charge is £10 per request irrespective of how much Information is requested.

Applicants are able to request specific Information or all the Information held. The Information requested may be held electronically or in manual files and

includes expressions of intent or opinions as well as factual information. It may include (but is not limited to) such formats as emails, letters, photographs and call recordings.

Information must be provided to the Applicant within 40 calendar days of the receipt of a SAR, as long as the Applicant has provided sufficient Information, the required fee and any confirmation of identity required. (The time frame for providing information to Applicants is set by legislation and may be subject to change.)

Information must not be destroyed, altered or concealed in order to prevent it being provided. However, routine amendments and deletions that would have taken place in any event should continue unless there is a specific reason to prevent this (e.g. a piece of Information that would have been deleted has specifically been requested).

The DPA creates a general right of access to Information of which the applicant is the Data Subject. It does not provide a right of access to Information about Third Parties unless certain conditions are met. There are circumstances under which the Information may need to be withheld, such as Information that is being processed for the prevention or detection of crime and where provision of this Information would prejudice the investigation, for example where the applicant making the request is under investigation for possible fraud. Other circumstances include disclosing Information that would be prejudicial to negotiations underway with the applicant (for example over a claim for Costs or other redress) and Information covered by legal professional privilege. If a request is being made by someone else on the applicant's behalf, for example, a carer on behalf of a disabled person, or an appointed legal representative, they will need to provide proof that they have appropriate authority. A SAR can be made as part of a Complaint or Appeal. The Service Provider shall prescribe a process to recognise such requests and respond to them.

Requests that include a Complaint about Data Protection or a request to exercise another right under the DPA should be recognised and handled according to the Data Protection Complaints procedure agreed with GLA. This includes the three scenarios outlined below.

- Under section 10 of the DPA, an individual is entitled to give written notice (known as a Data Subject Notice) at any time to require the Data Controller to cease, or not to begin Processing any Personal Data where the Processing of that Data is causing or would be likely to cause substantial damage or distress, to themselves or another.
- Under section 11 of the DPA, an individual is entitled to give written notice at any time to require the Data Controller to cease, or not to begin, the Processing of Personal Data of which that individual is the Data Subject, for the purposes of direct marketing. In this case, the term direct marketing means the communication – by any means - of any advertising or marketing material that is directed towards particular individuals.
- Under section 12 of the DPA, an individual is entitled to give written notice at any time to require a Data Controller to ensure that no decision taken by

or on behalf of the Data Controller is based solely on an automated means of Processing Personal Data.

Note that individuals that are sole traders or partnerships are protected by the Data Protection Act; companies are not.

2.4 Responsibilities

The Service Provider's role is:

- to implement a procedure to handle SARs within the time limits and stipulated by the DPA;
- to implement a procedure to handle requests from individuals to exercise their rights under sections 10 – 12 inclusive of the DPA;
- to ensure that there is at all times a member of the Service Provider's Personnel with sufficient seniority and understanding to manage SARs;
- to ensure that all Personnel are trained to recognise a SAR and know what they should do when one is identified;
- where the Service Provider (or any Sub-Contractor) is sending a response direct to the applicant who has made a SAR, the response must be provided to the applicant within the statutory timeframe, which is currently 40 calendar days of their request having been received (wherever the request was initially received);
- to report to GLA on the number of requests received; and
- to liaise with GLA on any Complaints or policy issues arising in connection with SARs.

Forms & Letters & Other Materials

- The Service Provider should devise a form to help applicants to make a SAR. The form should be made available in hardcopy format and in soft copy format on the Services Website.
- Individuals who provide all the necessary Information, confirmation of identity and the required fee by other means should not be required to fill out a form.
- The Service Provider shall devise letters that are to be used in connection with SARs.
- The Service Provider shall produce a list of explanations of codes, abbreviations and terms that are not explained elsewhere.
- The Service Provider shall provide the Privacy Notice and a list of possible sources and recipients of Information held. This should be included with each response to a SAR.

2.5 Systems

As far as feasible, these should be electronic and minimise manual / paper-based processes.

The Appeal Service System(s) shall be capable of processing and recording payments for SARs but must not *require* a payment in order to progress a request. The Appeal Service System(s) shall be capable of logging and

tracking requests to ensure they are fulfilled within the timescales stipulated by the DPA; to support reporting and to allow auditing and support investigation should a Complaint about the handling of a request be received. The Service Provider shall keep an up-to-date log of all Data repositories to ensure that it can perform a complete search when a request asks for 'all Information'.

The Appeal Service System(s) shall provide automated search, retrieval and printing functionality for all personal Information repositories. This is to minimise the manual effort involved in processing requests.

The Appeal Service System(s) shall provide the ability to search a call recording platform and provide Data in CD-ROM or other suitable format to allow Customer to play back.

2.6 Processes

The Service Provider shall train Personnel on how to recognise an initial request and how to advise the Applicant on progressing it. The request may be received by the Contact Centre, via a Web enquiry form or by post. The request may be on its own or combined with a request, Complaint or other communication.

The Service Provider shall have a procedure for sending out SAR forms to enquirers or directing them to the soft copy on the Service's Website as appropriate. The Service Provider shall also have a procedure for dealing with requests in other formats and requests that do not contain the required information or fee.

The Service Provider shall develop a process for checking requests to ensure they contain all required information, including sufficient information to confirm identity and the fee required.

The Service Provider shall develop a process to provide any retrieved Information to Applicants in either hard copy format or 'paper free' format for example on a CD-R or wave file.

2.7 Reporting

The Appeal Service System(s) shall support GLA's reporting requirements as outlined within this Appendix and in accordance to the Service Level Agreement.

2.8 Checklist

The checklist in Table 1 gives step-by-step guidance on handling SARs. This shall be reflected in the procedure implemented by the Service Provider.

Table 1: SAR checklist

Trigger	Action	Requirements
Individual asks how they can get a copy of their personal information (either specific information or all information)	▪ Recognise request and advise applicant how they can progress it ▪ Advise that request must be in writing ▪ Recognise if sufficient information and payment is already provided by the applicant	▪ Staff training
SAR received – either using form or by other means e.g. letter	Scan into Appeal Service System(s) and direct to correct queue	▪ Specific work queue assigned to SARs ▪ Designated staff to Process SARs
Check request is complete	▪ Check that sufficient information is provided ▪ Check that payment is provided ▪ Check that copies of identity documents have been provided ▪ Check that request is for Information held by the Service Provider ▪ Check whether that request is part of a campaign or a repeat request Note - a request for Information is not a repeat request where new Information has been added to the System since the last request, or where a reasonable period of time has elapsed since their last request, e.g. three (3) Months	▪ Payment processing functionality - that also supports progression of the request without payment ▪ Logging and tracking functionality for SARs ▪ Ability to suspend timeline where further information / fee / clarification is required ▪ Ability to send communication to Customer to request missing information/payment ▪ Ability to reject SAR where necessary

Trigger	Action	Requirements
Start search for information	▪ Recognise if request is for 'all' or specific Information ▪ Recognise if there is a policy issue that needs referral to GLA	▪ Automated search functionality ▪ Ability to send out a letter to the Customer acknowledging receipt of their request ▪ Clear escalation procedures
Track request	▪ Track the request to ensure that it is progressing within the stipulated timescales ▪ Check for problems or logjams	Logging and tracking functionality Ability to send a letter to customer to advise if final response is going to be late (i.e. longer that the stipulated timescales)
Compile Information	▪ Print out Information and check it is complete ▪ Chase up any missing Information ▪ Check call recording database if applicable and download call to suitable media.	Secure storage for Information in hardcopy Secure storage / restricted access for Information in electronic format.
Check Information	▪ Check Information matches request ▪ Check details of Customer or their Vehicle in the Information match those in the SAR ▪ Check for Information about Third Parties and 'redact' or otherwise to remove this. ▪ Check for any other Information that should not be disclosed because it is covered by an exemption (e.g. Information relating to an investigation of the Customer where this would be prejudiced by the provision of the Information) ▪ Customise letter to send out with the material	▪ Ability to produce letter/email and print it out locally so that it can be added to the information retrieved ▪ Ability to add free text to the letter/email where necessary ▪ Ability to send Information in format specifically requested by the Applicant (for example on CD-R rather than hard copy) or wave file to be sent by email

Trigger	Action	Requirements
Record Information supplied	Record what Information was supplied to the Applicant. This is in case of Complaints that not all Information requested was supplied.	Ability to record what Information was supplied to the Customer and to retain a copy for the period stipulated in the Data Retention Policy
Dispatch Information	▪ The response should be sent out by Special delivery and marked 'Private & Confidential - Addressee only'. The response should be sent first class if there are less than five (5) days until the statutory deadline is reached (this is in case of Complaints received that the Information was not received)	Ability to send out the response using chosen method of post or email.

3 Information Access Request Procedure

3.1 Background

This section refers to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) which give the public the right of access to Information held by public authorities, of which GLA is one.

EIR specifically govern the disclosure of Information relating to the environment, broadly defined as:

- information relating to the state of the elements of the environment, and the interaction of these elements;
- information relating to factors affecting or likely to affect the elements of the environment;
- measures, including administrative measures, and activities affecting or likely to affect the elements and factors referred to above, and measures or activities designed to protected those elements;
- reports on the implementation of environmental Legislation;
- cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to above; and
- the state of human health and safety.

FOIA governs the disclosure of all other Information, other than Personal Data disclosed to the Data Subject, which is covered by section 7 of the DPA as described above.

Under both pieces of Legislation, the public authority has a duty to confirm or deny whether or not the requested Information is held; and to supply a copy of the Information if it is held unless an exemption applies.

Requests for information made under FOIA must be made in a permanent format. This may include by letter or email. The public authority has a duty to advise and assist anyone contacting it (or their Contractors) to ask how to request information.

Requests for information received under EIR can be made verbally as well as in writing. However, a process should be in place to enable Customer Service Representatives to record a written copy of the request.

Valid requests for information under FOIA and EIR should:

- Make a request for information; and
- Include a name and address for response (this can simply be an email address).

There is no obligation for Applicants to prove their identity, use their real name, mention FOIA or EIR or disclose why they want the information requested.

Information held by any Service Provider or Contractor or Sub-Contractor in relation to a contract with the public authority is also subject to public access. This includes successful and unsuccessful tenders relating to contracts.

The Service Provider shall be aware that any documents that have been protectively marked as 'confidential' or 'commercial in confidence' will not necessarily prevent disclosure under FOIA or EIR.

It is a criminal offence under FOIA to alter, conceal or destroy Information with the intention of preventing the disclosure of that Information to an applicant. However, routine amendments and deletions that would have taken place in any event should continue unless there is a specific reason to prevent this (e.g. a piece of Information that would have been deleted has specifically been requested).

Where information requested relates to the applicant themselves, then the applicant shall be advised to make a SAR under the DPA.

Final responses to FOIA and EIR requests must be supplied within twenty (20) Working Days of a request being received by the public authority (or its service providers or Contractors).

Under FOIA, exemptions can be applied to some Information to prevent disclosure but many exemptions are subject to a 'public interest' test where the authority must consider whether it is more in the public interest to supply or withhold the Information.

Under EIR, exceptions can be applied to some Information to withhold disclosure. All exemptions are subject to public interest considerations and the authority must consider whether it is more in the public interest to supply or withhold the Information.

3.2 Responsibilities

The Service Provider will be responsible for:

- responding to requests under FOIA and EIR;
- determining whether exemptions or exceptions are to be applied;
- applying the 'public interest' test;
- determining whether or not the cost limit has been reached and whether or not to proceed with the request;
- consulting with GLA, Third Parties, or TfL , as necessary, prior to disclosing Information under the Legislation; and
- handling the Complaints procedure and any requests for review.

The Service Provider shall:

- train its staff to recognise requests made under FOIA and EIR and the process they should follow, even when those requests are included in other correspondence, such as Notices of Appeal;
- train staff to distinguish between requests to be handled in this way and business as usual correspondence have a designated member of staff at all times who will ensure the Service Provider's compliance with requirements in relation to FOIA and EIR;
- provide guidance to the public where a request can be satisfied by Information that is already published;
- respond to all requests from GLA for the provision of Information required to satisfy a request within the required timescale and as

may be specified by the relevant Performance Indicators found in this Agreement);

- inform GLA of the staff costs involved in retrieving the Information - if over £450 (based on eighteen (18) hours of work in retrieving, locating, or redacting the Information), public authority is entitled to charge the requester the full cost over this amount; and
- provide reasonable advice and assistance to Customers unable to make a request in writing.

For avoidance of doubt, no additional costs will be paid to the Service Provider for handling the retrieval of information in response to FOIA or EIR requests, even if the costs exceed £450.

FOIA or EIR requests can be made as part of general correspondence, Complaint or Appeal. The Service Provider shall prescribe a process to recognise such requests and respond to them.

3.3 Systems

The Service Provider shall ensure that its Systems can support the retrieval of information requested under FOIA and EIR within the required timescales.

The Service Provider's Systems shall support the retrieval and presentation of the Information in a suitable format required by GLA.

Should the Information already be available via the MIS, it is likely it will be taken from there. However, there may be requests for other Information that is not held in the MIS.

Information does not have to be manipulated or restructured if it is not held in the format the person has requested. But the raw Information that pertains to their request will need to be supplied. However, raw Information may often need to be redacted or restructured to prevent the undesirable disclosure of Information where an exemption or exception applies, or is outside the scope of a request.

The Service Provider shall supply the Information to GLA in full even if the Service Provider believes an exemption may apply. GLA will determine whether this is the case.

The Service Provider shall have logging, tracking and reporting functionality in place to ensure it meets its obligations in respect of FOIA and EIR requests.

3.4 Processes

The Service Provider shall have a process in place to ensure it:

- recognises FOIA and EIR requests;
- forwards FOIA and EIR requests to GLA which are appropriate to GLA;
- supplies Information requested by GLA to respond to a FOIA or EIR request; and
- records its actions to meet reporting requirements.

3.5 Reporting

The Service Provider shall report to GLA in relation to FOIA and EIR requests in accordance with the Service Level Agreement.

3.6 Checklists

The checklist gives step-by-step guidance on dealing with FOIA and EIR Requests. This shall be reflected in procedures to support this implemented by the Service Provider.

Table 2: FOIA/EIR checklist

Trigger	Action	Requirements
Individual contacts the Service Provider, making a request for information under FOIA or EIR	▪ Request is recognised as a request under FOIA or EIR (whether the person states this or not) ▪ Requests received are logged	▪ Training for staff ▪ Designated member of staff to oversee the Service Provider's compliance with their obligations and GLA requirements in relation to FOIA and EIR ▪ Logging, tracking and reporting functionality

1. INFORMATION GOVERNANCE

1.1 Information Governance

This section covers the generic Requirements applicable to the Service Provider in relation to Information Governance. These Requirements include but are not limited to the following:

- Generic requirements;
- Data Protection requirements;
- Data Protection audit;
- Reporting of breaches of Privacy Legislation;
- Subject Access Request(s);
- Information Access Request(s);
- Contractors;
- Complaints.

1.2 Data Retention

Z 1.2.1		Mandatory
The Service Provider shall comply with all GLA's specific Requirements relating to retention periods for all Data as specified in Appendix 2: Data Retention and Information Record Disposal. Where no period has been specified, the Data will be retained for as long as is required for the purpose for which it was collected, and no longer in accordance with Appendix 2: Data Retention and Information Record Disposal.		

Z 1.2.2		Mandatory
The Service Provider shall securely delete all Data at the expiry of its retention period, in accordance with Appendix 2: Data Retention and Information Record Disposal.		

Z 1.2.3		Mandatory

The Service Provider shall ensure that all Data deleted at the expiry of its retention period cannot be accessed by anyone. Data held on paper shall be securely shredded and Data held electronically shall be deleted using tested deletion scripts in accordance with this Statement of Requirements.

Z 1.2.4		Mandatory
The Service Provider shall use industry standard disk-wipe Software and other mechanisms in accordance with this Statement of Requirements to make unusable all media that are no longer operational. This includes optical disks, floppy disks, hard disk drives, solid state storage, paper and tapes. This process of securely erasing media shall be documented and tested, and shall include the production of certificates of destruction as required by GLA.		

Z 1.2.5		Mandatory
The Service Provider shall ensure that the Appeal Service System(s) has the functionality to protect Data from automatic deletion in the event that it is required for further reference.		

Z 1.2.6		Mandatory
The Service Provider shall ensure that the Appeal Service System(s) has the functionality to remove the protection on Data so that the Data can be destroyed in accordance with Appendix 2: Data Retention and Information Record Disposal.		

Z 1.2.7		Mandatory
The Service Provider shall provide GLA with certificates of destruction when Data is deleted.		

1.3 Data Protection

Z 1.3.1		Mandatory
The Service Provider shall submit to GLA for Approval and, when Approved comply		

with, a mechanism for the validation of Data at the point such Data is entered into the Appeal Service System(s).

Z 1.3.2		Mandatory
The Service Provider shall ensure that all Data Stores comply with this Statement of Requirements and Appendix 2: Data Retention and Information Record Disposal.		

Z 1.3.3		Mandatory
The Service Provider shall collect and process Personal Data only in accordance with the instructions and directions given by GLA and in accordance with Privacy Legislation.		

Z 1.3.4		Mandatory
The Service Provider shall store and Process all Personal Data, with the exception of DVLA Data, within the European Economic Area (EEA). The storing and Processing of Personal Data outside of the EEA is prohibited. For avoidance of doubt, Processing shall include (but is not limited to) the ability to read the data.		

Z 1.3.5		Mandatory
The Service Provider shall not store or access any Data including any provided by the DVLA through the Appeal process outside the United Kingdom (UK) save to the extent agreed by the Parties in accordance with the Change Control Request Procedure (such procedure may involve associated discussions with the DVLA).		

Z 1.3.6		Mandatory
The Service Provider shall protect all Personal Data against unauthorised and unlawful Processing, accidental loss, alteration, destruction and damage in accordance with Privacy Legislation.		

Z 1.3.7		Mandatory
The Service Provider shall develop and agree a suitable Privacy Notice with GLA.		

Z 1.3.8		Mandatory
The Service Provider shall ensure that the Privacy Notice is updated upon request by GLA within five (5) days of such request at no cost to GLA.		

Z 1.3.9		Mandatory
The Service Provider shall ensure that the Appeal Service System(s) shall issue a Privacy Notice to any Customer on request by the Customer.		

Z 1.3.10		Mandatory
The Service Provider shall develop and comply with a mechanism for Customer identification checks before any Data amendments are carried out and shall submit such a mechanism to GLA for Assurance.		

Z 1.3.11		Mandatory
The Service Provider shall ensure that where the Appeal Service have to revert to manual workaround processes, that adequate measures and controls are in place to protect the Data against misuse and loss in accordance with Privacy Legislation and PCI DSS regulations.		

Z 1.3.12		Mandatory
The Service Provider shall develop and comply with processes to enable controls to be placed on postal activities to guarantee receipts are processed daily and are not misplaced and misallocated and shall submit such processes to GLA for Assurance prior to the Operational Commencement Date.		

Z 1.3.13		Mandatory
The Service Provider shall handle any Data, including Personal Data, according to the classification specified by GLA.		

Z 1.3.14		Mandatory
The Service Provider shall notify GLA within five (5) days of all changes to all		

processes and activities (including locations where they may be undertaken) that will require GLA to update its Notification on the ICO Register of Data Controllers.

Z 1.3.15		Mandatory
The Service Provider shall ensure all VRM(s) are treated as Personal Data.		

Z 1.3.16		Mandatory
The Service Provider shall ensure that controls are in place to prevent the copying, reproduction and removal of Data in accordance with Privacy Legislation and PCI DSS regulations.		

1.4 Data Protection Audit

Z 1.4.1		Mandatory
The Service Provider shall submit to GLA for Approval, and when Approved comply with, a Data Protection Audit Plan. The plan shall include: • timescales for preparation and conduct of the annual audit; • the audit strategy and planned outputs; and • details of the independent Third Party undertaking the audit.		

Z 1.4.2		Mandatory
The Service Provider shall comply with the Data Protection Audit Plan.		

Z 1.4.3		Mandatory
The Service Provider shall ensure that a comprehensive Data Protection audit is carried out by an independent Third Party at no cost to GLA. Details of the proposed Third Party must be submitted to GLA for Approval prior to the audit being carried out.		

Z 1.4.4		Mandatory
The Service Provider shall undertake a Data Protection audit every twelve (12)		

months (or such other frequency as GLA may require) and report the findings to GLA.

Z 1.4.5		Mandatory
The Service Provider shall implement any recommendations from any Data Protection audits within timescales set by GLA.		

1.5 Reporting of Data Protection Breaches

Z 1.5.1		Mandatory
The Service Provider shall report all breaches of Privacy Legislation and all other Data security incidents to GLA within one (1) Working Day.		

1.6 Evidence

Z 1.6.1		Mandatory
The Service Provider shall ensure that the Evidence Data is treated as “OFFICIAL”, from an integrity perspective, as defined under the UK Government Protective Marking Scheme (GPMS).		

Z 1.6.2		Mandatory
The Service Provider shall develop and comply with processes that ensure that the transmission of Documents and Appeal Evidence Data over a public network is done securely in accordance with security measures equivalent to those used by major financial institutions for the protection of financial data and shall submit such processes to GLA for Assurance.		

Z 1.6.3		Mandatory
The Service Provider shall allow Authorised Users to access and retrieve Evidence.		

Z 1.6.4		Mandatory
The Service Provider shall ensure that it stores any and all Documents and Evidence		

in accordance with GLA's security requirements as specified in the General Statement of Requirements.

Z 1.6.5		Mandatory
The Service Provider shall ensure that relevant access to Evidence is recorded and stored for audit purposes including, without limitation, who accessed it and the date and time that it was accessed.		

1.7 Subject Access Requests (SARs)

Z 1.7.1		Mandatory
The Service Provider shall submit to GLA for Approval prior to the Operational Commencement Date, and when Approved comply with, a procedure for processing SARs in accordance with Privacy Legislation.		

Z 1.7.2		Mandatory
The Service Provider shall ensure that its Appeal Service System(s) has functionality to process, retrieve and print SAR information sourced from the Appeal Service System(s).		

Z 1.7.3		Mandatory
The Service Provider shall ensure that Call Recordings can be to be transferred and transmitted to Customers by electronic media as they may form part of a SAR.		

Z 1.7.4		Mandatory
The Service Provider shall ensure that a SAR response can be issued to a Customer in either hard copy or electronic format if requested to do so by either the Customer or GLA.		

Z 1.7.5		Mandatory
The Service Provider shall ensure that the Appeal Service System(s) has functionality		

to handle an administration fee for the purpose of SARs or any other request or service which GLA determines should attract an administration fee.

Z 1.7.6		Mandatory
The Service Provider shall submit to GLA for Approval and, when Approved comply with, a procedure to deal with SAR requests where the Customer is unable to provide written correspondence. For the avoidance of doubt written correspondence shall include but not be limited to email.		

1.8 Freedom of Information (FOI) Requests

Z 1.8.1		Mandatory
The Service Provider shall submit to GLA for Approval prior to the Operational Commencement Date, and when Approved comply with, a process on how to respond to FOI requests. Such proposed processes are to include (but are not limited to) a format for presenting to the Customer any relevant Data surrounding the Freedom of Information Request (e.g. Data table, graphical representation, copy of Document etc).		

Z 1.8.2		Mandatory
The Service Provider shall submit to GLA for Approval and, when Approved comply with, a procedure to deal with FOI requests where the Customer is unable to provide written correspondence. For the avoidance of doubt written correspondence shall include but not be limited to email.		

1.9 Environmental Information Regulations (EIR) Requests

Z 1.9.1		Mandatory
The Service Provider shall submit to GLA for Approval prior to the Operational Commencement Date, and when Approved comply with, a process on how to respond		

to EIR requests. Such proposed processes are to include (but are not limited to) a format for presenting to the Customer any relevant Data surrounding the EIR requests (e.g. Data table, graphical representation, copy of Document etc).

Z 1.9.2		Mandatory
The Service Provider shall submit to GLA for Approval and, when Approved comply with, a procedure to deal with EIR requests where such a request is made verbally.		

1.10 Contractors

Z 1.10.1		Mandatory
The Service Provider shall ensure that any of its Contractors and Sub-Contractors engaged in providing any part of Appeal Service are aware of, and comply with, their obligations under the Data Protection Act 1998, the Freedom of Information Act 2000, the Environment Information Regulations 2004 and any other applicable Legislation.		

1.11 Complaints

Z 1.11.1		Mandatory
The Service Provider shall submit to GLA for Approval prior to the Operational Commencement Date, and when Approved comply with, a process on how to respond to the following types of Complaints: • those made under sections 10 -12 of the Data Protection Act 1998 • those made to the Service Provider about how a request for Information was handled.		

Z 1.11.2		Mandatory
The Service Provider shall notify GLA within one (1) Working Day of receipt of any complaints submitted to the Information Commissioner's Office regarding an Information request or Complaint made about the Appeal Service. For the avoidance		

of doubt, this includes all requests processed by the Service Provider, its Contractors and/or its Sub-Contractors.