Information governance and data protection standards for data processors

This delivery of this service will involve the provision of services to the Greater London Authority (GLA) that will require a supplier to process personal data on our behalf.

The Data Protection Act 1998 imposes certain requirements on the GLA in relation to the selection and use of its data processors. To help us fulfil these requirements, you must, as a potential data processor on behalf of the GLA, provide certain information to us so that we can determine whether you can provide sufficient guarantees in relation to the processing and an appropriate level of security for the personal data. The GLA reserves the right to assess your service at any time regarding your ability to provide these guarantees using the questionnaire below – your service must be able to satisfactorily complete this questionnaire or be at risk of default on your contract.

YOUR DETAILS	
Organisation name	THAMES REACH HOUSING ASSOCIATION
Address	The Employment Academy 29 Peckham Road London SE5 8UA
Contact name	███████████
Contact details	Telephone: ███████████
	Fax: ███████████
	Email: ███████████████████

YOUR SECURITY POLICIES AND PROCEDURES		
Do you have a current Notification in the Information Commissioner's Register of Data Controllers? If yes, please supply a copy	Yes [✓]	No [_]
If you answered no to the question above, is your processing exempt from Notification?	Yes [_]	No [_]
Do you have an information security policy? If yes, please provide a copy	Yes [✓]	No [_]

Does your information security policy include the following:				
-- physical security of premises and processing areas	Yes	[✓]	No	[_]
-- physical entry controls	Yes	[✓]	No	[_]
-- equipment security and maintenance	Yes	[✓]	No	[_]
-- password and access controls	Yes	[✓]	No	[_]
-- security of mobile equipment and devices (e.g. laptops, memory sticks, PDAs)	Yes	[✓]	No	[_]
-- controls against malicious software	Yes	[✓]	No	[_]
- encryption	Yes	[✓]	No	[_]
-- business continuity planning	Yes	[✓]	No	[_]
- monitoring system access and use (including audit trails)	Yes	[✓]	No	[_]
- management and mitigation of security incidents	Yes	[✓]	No	[_]
Does your information security policy comply with ISO 27001 (formerly BS 7799)? ██████████████████████████████ ███████████████████	Yes	[_]	No	[✓]
Do you have a policy for complying with the Data Protection Act 1998? If yes, please provide a copy ███████████████████████████ ████████████	Yes	[✓]	No	[_]
Do you have a clear desk policy? ███████████████████████████████ ████████████████████████████ ███████████████	Yes	[✓]	No	[_]
Do you have a clear screen policy? Included in Information Sharing and Confidentiality Policy	Yes	[✓]	No	[_]
Do you audit compliance of your information security and data protection policies?	Yes	[✓]	No	[_]

Do you have a secure disposal policy for equipment, media and data?   Yes [✓]   No [_]

If yes, please provide a copy

██████████████████████████████████

███████████████████████████████████████

██████████████████████████████████████

████████████████████████████████████

██

███████████████████████████████████████

Please describe how you dispose of paper records:

██

███

██

█████████████████████████

Describe the measures you have in place to prevent unauthorised access to your systems from outside your company:

██

█████████████████████████████████████

██

████

██

Do you have a back up and disaster recovery policy?   Yes [✓]   No [_]

If yes, please provide a copy

███████████████████████████████████

███████████████████████████████████

███████████████████████████████████

████████████████████████████████████

███████████████████████████████████

████████████████████████████

█████████████████████████████

█████████████████████

Please indicate what virus detection and prevention software you use:

██

Do you store, or otherwise process, any personal data off-site?	Yes [✓] No [_]

If yes, please provide details

████████████████████████████████████

████████████████████████

███████████████████████████████████

██████████████████████████████

██████████████████████████████

████████████████████████████████████

███████████████

Will you process any personal data outside the European Economic Area as part of the provision of services to the GLA?

██

███

██

██

████████████████████████

YOUR EMPLOYEES	
Do you carry out verification checks on all potential employees?	Yes [✓] No [_]
Do you have a personnel screening and vetting policy? If yes, please provide a copy ████████████████████████████████ ██████████████████████	Yes [✓] No [_]
Do you ensure the reliability of employees who process personal data? If yes, please provide details: ████████████████████████████ ████████████████████████████ ██████████████████████████ ██████████████████████████ ████████████████████████ ████████████████████████ ████████████████	Yes [✓] No [_]
Do you train staff on the care and handling of personal data and	Yes [_] No [_]

information security?

If yes, please describe what this training involves:

████████████████████████████████████

███████████████████████████████

███████████████████████████████

██████████████████████████████

██████████████████████████████

███████

██████████████████████████████

███████████████████████████████

████████████

Do your contracts with your employees include:		
-- confidentiality clauses?	Yes [✓]	No [_]
-- obligation to comply with information security and data protection policies?	Yes [✓]	No [_]

YOUR CONTRACTORS* (*this means any third party you appoint to process personal data as part of your delivery of services)		
Do your contractors sign confidentiality agreements before accessing your systems?	Yes [✓]	No [_]
Will you use sub-contractors to assist with the processing services for the GLA? If yes, please provide details of the contractual arrangements you have in place with them:	Yes [_]	No [✓]

Have you taken steps to ensure that any sub-processors you will use to assist you with the processing services for the GLA have appropriate security measures in place for the personal data?	Yes [_] No [_]
If yes, are you satisfied that the personal data will be adequately protected if you use these sub-processors?	Yes [_] No [_]
Do the contracts you have with your sub-contractors impose obligations upon them to observe confidentiality and security in relation to any personal data which they may be required to process?	Yes [_] No [_]
Will your contractors process any personal data outside the European Economic Area as part of the provision of services to the GLA? If yes, please provide details	

YOUR ASSURANCE

Has your processing of personal data ever been the subject of any complaints to the Information Commissioner, or any other regulator? If yes, please provide details:	Yes [_] No [✓]
Have you ever had a security breach resulting in loss or unauthorised disclosure of personal data? If yes, please provide details:	Yes [_] No [✓]