Data Sharing Agreement for elector name and addresses for the 2024 GLA election between

Each London Borough (inc City of London Corporation)

And

Greater London Authority

Contents

1. Introduction to the Sharing

This Data Sharing Agreement [DSA] documents how the parties to this agreement will share personal data with the Greater London Authority (GLA) (directly to their contractor PSL Ltd) to meet a legal requirement in the London Government Representation Of The People, The Greater London Authority Elections (Election Addresses) Order 2003. By signing this Agreement via ISG, the Parties agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal Data to be shared.
- Set out the lawful basis conditions under UK GDPR and Data Protection Act 2018 through which the information is shared.
- Stipulate the roles and procedures that will support the processing/sharing of information.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

1.1. Partner / Parties

For simplicity, the Partner Organisation will be referred to as ‘Partner’. The Parties are the GLA and each London Borough Council inc the City of London.

1.2. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act.

All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights and complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement

and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.

- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Manager if they are unsure at any point in the processing and sharing of personal data.

1.3. Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks and DBS checks.

1.4. Assessment, review, and Termination of agreement

This is a one off agreement for the May 2024 London elections.

2. Purpose and Benefits

2.1. Purpose

This agreement covers the sharing of information by the individual London Boroughs to the GLA under Rule 9 of London Government Representation Of The People, The Greater London Authority Elections (Election Addresses) Order 2003. That specifies that the Greater London Returning Officer shall ensure that a copy of an election booklet is addressed and delivered to each elector in the election at the GLA's expense. The Order sets out details about which candidates are entitled to have election addresses contained in the booklet and various formalities about costs and contents. There is therefore a legal duty for GLA to cause a booklet to be sent to each elector. Each London Borough must provide the GLA with the names and full postal address of each registered elector in its borough to enable the GLA to meet its legal requirements.

GLA have subcontracted a data processor- PSL Ltd - to undertake the printing and posting of the booklets. Therefore the name and address of each elector must be shared by the relevant council with the GLA, straight to the GLA's data processor PSL Ltd.

PSL will send the booklet to each registered elector. This will be done in batches as is required by the GLA for example postal voters will receive a copy in a first batch as they can vote before polling day. Therefore Boroughs will provide the data to the GLA (to PSL ltd) in batches as required by GLA.

2.2. Benefits

The sharing will enable the GLA to meet its legal requirements. It will improve democratic engagement by the electorate. Sharing directly with the sub-contractor will prevent unnecessary processing by the GLA, although the GLA remain Data Controller on receipt.

2.3. Lawful Basis

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements.

The legal basis is Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject. The law is the London Government Representation Of The People, The Greater London Authority Elections (Election Addresses) Order 2003, rule 9. If individual London Boroughs consider that this legal basis does not cover them, then the legal basis would be Article 6(1)(e) public task, with the underlying law being the same as above, and sharing being necessary to allow the GLA to meet its legal obligations.

No special category or criminal offence data is shared.

2.4. Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) as the lawful basis condition used for processing under this agreement. Consent is not the lawful basis for processing information shared under this agreement.

2.5. Proportionality and necessity

Proportionality, data minimization, necessity and not being excessive are factors to be taken into consideration when deciding whether to share personal information. These requirements are met by this sharing.

2.6. Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority. Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who received the request as the legal duty lies with them. In order to ensure that the authority in receipt of the FOIA request is able to respond within the statutory deadline, any request for assistance or information made to partner authorities should be made and processed within two working days, and any data exchange completed within seven working days.

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Given the low level and non-sensitive nature of the data and the purpose of processing it is not considered that a DPIA is necessary, although given the overall volume of data being processed, a short form risk assessment has been undertaken to explain why the processing is low risk.

3.1. Right to be informed – Privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UK GDPR and will make any necessary amendments to their existing Privacy Notices.

3.2. Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of the organisation concerned.

3.3. Data subjects

The data subjects will be: registered electors in the 32 boroughs in London plus the City of London Corporation.

4. Data

4.1. The data to be shared

The data type that will be shared is name and postal address details, and by implication, the data subjects are over 18 and registered as an elector.

4.2. Storing and handling information securely

The information is to be shared directly with the GLA's subcontractor, PSL Ltd. PSL require information to be shared only by secure data upload. Their system has full Role Based Access Control and each submitting Borough will only be able to access their own folder, but not other authority's. PSL will provide each Electoral Registration Officer (or nominated officer) with their details for the system and a user guide as to how to upload the data securely.

PSL have undergone detailed data protection and information security due diligence checks (with the GLA's procurement process) which have been confirmed as being passed and completed. PSL Ltd have liability cover for up to £5m which will be sufficient cover.

4.3. Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted.

Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security such as NHS Digital's Data Security and Protection Toolkit (DSP) and Cyber Essentials or Cyber Essentials Plus.

4.4. Outside UK processing

No data is processed or shared outside the UK.

4.5. Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it shares and must have clear processes in place for managing data quality.

4.6. Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UK GDPR.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed and appropriate coordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.7. Retention and Disposal

The GLA's processor, PSL Ltd, will retain the data for 90 days after sending the booklets, to facilitate the processing of undelivered data. After that it will be securely deleted from their system.

Version control	
Document production date	16th January 2024
Document currency	0.4 draft