GREATER**LONDON**AUTHORITY

Personal Data Incident and Breach Policy

Date of approval and issue	17 May 2018
Document version	V1.0 – 17 May 2018
Changes from previous version	
Approved by	Governance Steering Group
Review date	April 2019

Senior owner	Executive Director of Resources
Document owner	Information Governance Manager and Data Protection Officer

Contents

Appendices

Preventing breaches

The effects of personal data losses are not only felt by the individuals concerned, but also affect the efficiency of the service and the reputation of the GLA.

It is important that all staff are aware of their responsibilities for handling personal information, keeping it secure and not disclosing it without proper cause. Senior Managers should ensure that all staff within their responsibility are familiar with the appropriate policies and procedures.

All data controllers have a responsibility to ensure appropriate and proportionate security of the personal data they hold. This is covered by the 6th principle of the General Data Protection Regulation (GDPR) as detailed below:

> 'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')'.

To prevent the GLA from being in breach of the requirements of the GDPR, all Assembly Members, staff (whether permanent or temporary) and all third parties acting on behalf of the GLA must be aware of their corporate and personal responsibilities set out under the provisions of the GDPR.

This policy must be read in line with GLA's Data Protection policy.

1. Purpose

1.1 The GLA has a duty under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, to ensure all personal data is kept safely and securely. We are committed to upholding the GDPR principles, managing the information we hold fairly and lawfully.

1.2 The potential for a personal data breach will always remain. The loss or misuse of personal information has the potential to impact significantly on individual rights and wellbeing and the reputation of the Authority. Furthermore, the Information Commissioner's Office (ICO) can impose significant fines on data controllers and to some extent, data processors which fail to identify and record data breaches and incidents, and which fail to notify the ICO within 72 hours of certain types of breaches being identified.

1.3 This policy describes the procedures and steps the GLA will follow in dealing with any breaches of personal data that may occur. It sets out a consistent approach and follows guidance provided by the ICO. In doing so, it seeks to ensure the GLA keeps to a minimum the impact of personal data breaches; and that the likelihood of breaches is minimised by ensuring lessons-learnt are promptly implemented across the organisation.

2. Scope

2.1 The GLA, each individual London Assembly Member and the Greater London Returning Officer (GLRO) are, for the purposes of the UK GDPR, the Data Protection Act 2018, and for the purposes of this policy, separately registered data controllers.

2.2 This policy applies to

a) all GLA employees and elected Members

b) any temporary, agency and contracted staff engaged by the Authority or working on behalf of the Authority, including staff working on behalf of Assembly Members and the GLRO in their capacities as separate data controllers to the GLA

c) any third parties who process personal data on behalf of the GLA (a data processor)

3. Roles and responsibilities

3.1 All staff and parties referenced in paragraph 2.2 above are responsible for ensuring personal data is managed in accordance with GLA policies and for reporting any data incidents or breaches immediately.

3.2 GLA Senior Managers will be responsible for ensuring operational compliance with this plan within their business areas and for seeking advice from the GLA Data Protection Officer when appropriate.

3.3 Senior Managers are also responsible for handling a breach within their area of responsibility and are required to take ownership of the breach (the breach owner) and the internal reporting and notification obligations covered in this policy.

3.4 The GLA Data Protection Officer (DPO) is responsible for providing advice and guidance regarding this policy and for keeping it up to date, in addition to specific roles and responsibilities referenced throughout this policy.

3.5 The Executive Director of Resources (as the GLA Senior Information Risk Owner) is the Senior Owner of this policy and has overall responsibility for the GLA's information risk policy.

3.6 This policy has been agreed and approved by the GLA Governance Steering Group.

3.7 This policy will be reviewed within one year of being implemented, and every three years thereafter, or earlier if necessary. Minor changes to this policy can be implemented by the GLA DPO, but all substantive amendments will be approved by either the Governance Steering Group or by the Executive Director of Resources.

4. What is a personal data breach?

4.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Breaches may involve either criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility. A breach is therefore more than just losing personal data.

4.2 Examples of breaches include:

- loss or theft of hard copy documents
- equipment failure
- loss or theft of equipment, which holds personal data, for example, laptops, tablets, CDs
- information obtained by underhand or deceptive means
- inappropriate or unlawful access, allowing unauthorised use
- human error
- unforeseen incidents such as flood or fire

- a hacking, phishing, smishing attack
- information being released inappropriately

Other examples of some of the most common personal data breaches are listed in Appendix 1 of this policy.

4.3 Breaches are also categorised according to the following three information security principles:

- A **confidentiality breach** is an unauthorised or accidental disclosure of, or access to, personal data
- An **availability breach** is an accidental or unauthorised loss of access to, or destruction of, personal data
- An **integrity breach** is an unauthorised or accidental alteration of personal data

5. Dealing with a breach

Identifying a breach has occurred

5.1 Under Article 33 of the GDPR, it is a legal requirement for the GLA to report certain data breaches to the ICO within 72 hours of the breach being identified. It is therefore imperative that all breaches involving personal data held or processed by the GLA are acted upon immediately.

5.2 Data processors and other parties who receive or handle GLA personal data must notify the GLA (or the appropriate data controller listed under paragraph 2.1) without undue delay and as soon as they become aware of a personal data breach.

5.3 The GLA will be regarded as having 'become aware' of a breach when it has a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised in manner outlined in paragraph 4.3 above. This puts an obligation on the GLA to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action.

5.4 The point at which the GLA can be 'aware' of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach of personal data, whereas in others, it may take some time to establish if personal data has been compromised (a potential data breach). Examples of how the GLA might become aware of a data breach are provided in Appendix 2 of this policy.

Reporting the breach

5.5 As soon as a breach has been identified, the officer concerned must report the incident immediately to their line manager, or the next senior officer.

5.6 A senior officer must at that point take responsibility for the breach and become the 'breach owner'. They should notify their relevant Head of Unit or Assistant Director and the GLA DPO.

5.7 Breaches involving data held or managed by or on behalf of Assembly Members must also be reported to the Executive Director or Assembly Secretariat.

5.8 If a breach of personal data occurs where the GLA is processing data on behalf of one of our partners, then the partner concerned must be notified immediately.

5.9 If a breach of personal data occurs from a partner organisation or party processing personal data on our behalf (a data processor) the effects of the breach on the GLA should be assessed and the use of this policy should be considered to protect the interests of the GLA, their customers and stakeholders. A Data Sharing agreement should be in place setting down breach reporting arrangements that are in line with this policy.

5.10 If a breach is suspected to have taken place, the following information must be provided to the GLA Data Protection Officer within 24 hours of the breach being identified:

- The type(s) of data involved
- An indication of how sensitive the data is
- Whether any protections were or are currently in place, for example, encryption
- How the breach occurred, how we found out about it, and who might now have access to the affected data
- What the data could tell a third party about an individual and what the potential impact is on the individual
- How many individuals' personal data are affected by the breach
- Who the individuals are whose data has been breached and what our relationship is with them
- How the data would put the privacy of those affected at risk, including if it will cause distress or physical harm
- The wider consequences to consider such as loss of public confidence, negative publicity, and financial implications
- The action that has been or is being taken to minimise the loss and its impact

Breach assessment

5.11 The GLA DPO will conduct a 'triage' assessment of the breach to assess the severity and impact of the breach and register it on the GLA Data Incident Log. This assessment will consider the nature of the breach, the sensitivity of the affected information and the potential impact on the individual(s) affected.

5.12 The GLA DPO will report the findings of the initial assessment to the following staff within 24 hours of the breach being reported to them:

- Head of Paid Service (if the initial assessment is the breach will need to be reported to the ICO)
- Executive Director – Resources (Senior Information Risk Owner)
- Executive Director of relevant directorate
- Assistant Director or Head of Unit for relevant team
- Head of Finance and Governance
- The reporting 'breach owner'

Recovery plan

5.13 Breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. Responsibility rests with the appropriate Executive Director, Assistant Director or Head of Unit in considering the action to be taken to:

- Protect the interests of the affected individuals
- Ensure the continuing delivery of the service
- Protect the interests of the GLA

5.14 The primary concern will be to establish whether losses can be recovered, and damage can be limited. The GLA DPO will help advise other areas of the GLA that need to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment, or simply changing access codes.

5.15 The GLA DPO will work with the 'breach owner' to fully assess the risk in terms of the potential adverse consequences for individuals; to ascertain how serious or substantial are the consequences and how likely are they to transpire.

6. Notifying the Information Commissioner's Office (ICO) and logging breaches

6.1 Article 33 of the GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office within 72 hours after having become aware of it. Where the notification to the ICO is not made within 72 hours, it must be accompanied by reasons for the delay. Failing to notify a breach when required to do so can result in a significant fine up to £17.5 million or 4% of the total annual turnover in the preceding financial year, whichever is higher.

6.2 In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries.

6.3 A personal data breach should be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This must be assessed on a case-by-case basis.

6.4 A recommendation on notification will be made by the GLA DPO after carrying out an assessment of the risks involved.

6.5 The decision as to whether to notify the ICO will normally rest with the Executive Director – Resources as the GLA Senior Information Risk Officer. Or, where this is not possible, with the Head of Paid Service.

6.6 If the decision is to notify the ICO, the GLA DPO will act as liaison with the ICO. The DPO will also ensure that the Executive Director – Resources and Head of Paid Service are informed of all reported breaches.

6.7 As a minimum, any notification to the ICO must include the following:

a) A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

b) the name and contact details of the Data Protection Officer or other contact point where more information can be obtained

c) A description of the likely consequences of the personal data breach (including the impact on the affected individuals)

d) A description of the measures taken, or proposed to be taken, by the GLA to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

6.8 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

6.9 The GLA shall document all personal data breaches regardless of their severity or the decision to notify the ICO. The Data Incident Log will record the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the GDPR.

6.10 Where the GLA is data processor for the affected personal data, reporting of the data breach must be done by the data controller. The GLA will provide full support to the data controller where required in mitigating the incident and especially if a report is being made to the ICO.

7. Informing individuals of a data breach

7.1 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the GLA must communicate details of the breach to the data subject(s) without undue delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage include, but are not limited to:

- discrimination
- identity theft or fraud
- financial loss
- damage to reputation
- a loss of confidentiality of personal data protected by professional secrecy

7.2 When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

7.3 Further information about assessing the risk to the data subject can be found in the Article 29 Guidelines on personal data breach notification under Regulation 2016/679 Section IV.

7.4 The GLA DPO will, as part of the 'triage' assessment process, make a recommendation, based on the conditions listed in paragraphs 7.1 to 7.3 above, as to whether the breach might result in a risk to the rights and freedoms of the affected individuals. This recommendation will be communicated to the relevant staff (listed under 5.12).

7.5 The decision to inform individuals of a breach involving their data will be made by the Executive Director of Resources, based on the recommendation of the GLA DPO and the views of the 'breach owner' or the appropriate senior management.

7.6 The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of paragraph 6.6.

7.7 The communication will be sent either by the GLA DPO, the 'breach owner', or a senior manager of the relevant GLA Directorate, depending on the severity of the breach and the nature of our existing relationship with the affected individuals. A decision will be made between the GLA DPO, the 'breach owner', and the relevant senior manager as to who would be the most appropriate signatory for that communication.

7.8 The affected data subjects may not need to be informed if any of the following conditions are met:

a) The GLA has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption

b) The GLA has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise

c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

7.9 The GLA may consider consulting the ICO to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

8. Post breach evaluation

8.1 Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on 'business as usual' will not be acceptable if systems, policies or allocation of responsibilities was found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and recorded so the GLA can be seen to have reacted in a responsible manner.

8.2 Those investigations into the cause of the loss of data should consider any staff capability or training issues that may be indicated and where appropriate, action may be considered under the GLA disciplinary procedure.

8.3 If the breach was caused, even in part, by systemic and ongoing problems, the GLA DPO will make recommendations on actions which will need to be taken and what procedures need to be in place to prevent any recurrence in the future.

9. Further reading

Article 29 Working Protection Working Party Guidelines on personal data breach notification under Regulation 2016/679 (GDPR)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

ICO Guide to the General Data Protection Regulation (GDPR) 'Personal data breaches'
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Appendix 1: Examples of common data breaches

Examples of some of the most common personal data breaches are listed below. Please note that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it, either verbally, in writing or electronically
- Computer infected by a virus or similar
- Finding data that has been changed by an unauthorised person
- Receiving and forwarding chain letters, including virus warnings, scam warnings and other emails which encourage the recipient to forward to others
- Unknown people asking for information which could gain them access to GLA data, for example, a password or details of a third party

Misuse

- Use of unapproved or unlicensed software on the GLA's equipment which results in access to a database, or part of a database, by someone not authorised to do so
- Sending a sensitive email to 'GLA All' or 'Local Gov Contacts All', or an unintended recipient
- Writing down your password and leaving it on display or somewhere easily found
- Printing or copying confidential information and not storing it correctly or confidentially

Theft or Loss

- Theft or loss of a hard copy file
- Theft or loss of any of the GLA's computer equipment

Appendix 2: Examples of becoming 'aware' of a data breach

- In the case of a loss of a USB drive with unencrypted personal data, it may not be possible to ascertain whether unauthorised persons gained access to data on that USB drive. Nevertheless, even though the GLA may not be able to establish if a confidentiality breach has taken place, such a case must be notified as there is a reasonable degree of certainty that an availability breach has occurred. The GLA would become 'aware' when it realised the USB key had been lost.

- A third party informs the GLA that they have accidentally received the personal data of one of its staff and provides evidence of the unauthorised disclosure. As the GLA has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become 'aware'.

- The TfL IT Shared Service detects that there has been a possible intrusion into its network. The GLA checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. The GLA became 'aware' once it had clear evidence a breach had occurred.

- A cybercriminal contacts the GLA after having hacked its system in order to ask for a ransom. After checking its systems to confirm it has been attacked, the GLA has clear evidence that a breach has occurred and there is no doubt that it has become 'aware' at that point.

Appendix 3: Definitions

Personal data means any information relating to an identified or identifiable living individual ('data subject')

Identifiable living individual means a living individual who can be identified, directly or indirectly, by reference to:

- an identifier such as a name, an identification number, location data or an online identifier, or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special category (sensitive) personal data

The UK GDPR singles out some types of personal data which are more sensitive and therefore require additional protection:

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**
- data concerning a person's **sexual orientation**

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject means the identified or identifiable living individual to whom personal data relates.

Appendix 4: Examples of personal data breaches and who to notify

Remember, all personal data breaches should be reported to **GLA Data Protection Officer** as soon as the breach is identified. The DPO will advise whether the ICO or the affected individual(s) should be notified about that breach and how notification will occur.

Example	Notify the GLA DPO	Notify the ICO	Notify the data subject	Notes
An encrypted USB drive is used to store a back-up copy of a spreadsheet containing the email addresses of those on a GLA mailing list. The USB drive is lost by a member of staff.	Yes.	No.	No.	If the data are encrypted, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
A GLA laptop suffers a ransomware attack which results in all data being encrypted. No back-ups are available, and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes.	Notification might be required if the laptop contained personal data that cannot be recovered or restored.	Only the individuals affected are notified if there is a high risk and others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.

Personal data of 5,000 GLA volunteers are mistakenly sent to the wrong mailing list with 200+ recipients.	Yes.	Yes.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in 'to' or 'cc' field, thereby enabling each recipient to see the email address of other recipients.	Yes.	Notifying the ICO may be obligatory if many individuals are affected, if sensitive data are revealed (for example, a mailing list of vulnerable people) or if other factors present high risks.	Yes, depending on the scope and personal data involved, but most recipients would already be aware their email address had been shared. The GLA should ensure it reassures those affected as a matter of good practice.	Notification may not be necessary if no sensitive data is revealed and if only a small number of email addresses are revealed.
A member of the public calls the GLA to report having received a job application letter intended for someone else. A short investigation establishes with reasonable confidence that a personal data breach has occurred.	Yes.	Yes.	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and we take the additional step of notifying other individuals if there is a high risk to them.