Appendix 12

PERSONAL DATA IN THE GLA GROUP

Executive Summary

The GLA Oversight Committee of the London Assembly is investigating the collection, use, storage, security and sharing of personal data across the GLA Group. The investigation will focus on four themes: using and sharing personal data, individual rights, security, and the future of personal data. The Committee is looking to publish a report in spring 2017, summarising the findings of its investigation and making recommendations to the Mayor and the functional bodies.

The functional areas of the GLA make extensive use of personal data for operational service delivery, with personal data shared for a range of purposes both within and outside of the GLA. The personal data sharing provided in the questionnaire responses is likely to represent only part of the actual sharing taking place within the GLA.

The GLA and its functional areas are subject to a number of data protection laws, but the introduction of the GDPR will be the most significant change in those laws in decades, and it is imperative that preparations are in place. GLA functional areas believe that they will be prepared for the GDPR by the time of its enforcement in May 2018, but the GLA should nevertheless consider a root and branch review of readiness for the GDPR, with central coordination and monitoring of readiness plans, and prepare contingency plans to mitigate areas where the GDPR's requirements might not be implemented by May 2018.

The UK's decision to leave the EU will not affect the applicability of the GDPR, and may introduce additional complexity for data protection management. The GLA has a role to provide central guidance on this for functional areas, and to prepare contingency arrangements should the UK's post-Brexit data protection environment not be considered to be equivalent to that of the GDPR.

In anticipation of the General Data Protection Regulation being enforced from May 2018, the GLA may wish to seek assurance of readiness from the functional areas, and in particular:

- prepare a comprehensive map of personal data use and register of controls;
- deliver initial GDPR training with annual updates;
- seek examples of good practice within the group and replicate or centralise these where appropriate (e.g. breach reporting processes);
- seek assurance that all functional areas have checked that where they use consent as a legal basis for processing, they have obtained and maintained a record of consent.

It should be noted that the bulk of the Metropolitan Police Service's processing is not based on consent from the data subject, and that in most cases personal data processed by MPS is subject to legislation other than the GDPR.

Whilst there is agreement that data protection is likely to become more complex over the next five years, there was no sense from the questionnaire responses that the functional areas may need to make fundamental changes to the way that data protection is managed in the GLA.

Introduction

Background

The GLA Oversight Committee of the London Assembly is investigating the collection, use, storage, security and sharing of personal data across the GLA Group. The investigation will focus on four themes: using and sharing personal data, individual rights, security, and the future of personal data. The Committee is looking to publish a report in spring 2017, summarising the findings of its investigation and making recommendations to the Mayor and the functional bodies.

Objectives

The objectives of the exercise include:

- to establish the protocols used across the GLA Group on the collection, use, storage, security and sharing of personal data.
- to identify good practice elsewhere and highlight any opportunities for the GLA Group to learn from.
- to establish the risks and opportunities of doing more or less sharing of personal data across the GLA Group.

Scope

The scope of the review includes the GLA and the functional bodies, specifically:

- Greater London Authority (GLA)
- London Fire and Emergency Planning Authority (LFEPA)
- London Legacy Development Corporation (LLDC)
- Mayor's Office for Policing and Crime (MOPAC)
- Metropolitan Police Service (MPS)
- Oak Park Development Corporation (OPDC)
- Transport for London (TfL)

Analysis was based upon the questionnaire responses and associated documentation, and did not include interviews or inspections.

Approach

The Committee wrote to the GLA and the functional bodies on 1st December 2016 to request information and key documents, to help inform the Committee's meeting on 23 February 2017. The request included a questionnaire to facilitate information gathering. The functional bodies were provided with support to complete the questionnaire, and responses were received at the end of January 2017.

Responses

All the functional bodies responded to the questionnaire, a copy of which is provided in Appendix A. The collated responses are provided in Appendix B, and a list of other documents provided is included in Appendix C.

Context

All analysis is based upon responses received to the questionnaire, and has not been verified through inspection or interviews. The GLA should seek a formal opinion of data protection practice before making operational decisions using the information in this report.

Using and Sharing Personal Data

Conclusions

The functional areas of the GLA make extensive use of personal data for operational service delivery, with personal data shared for a range of purposes both within and outside of the GLA. It should be noted that the bulk of the Metropolitan Police Service's processing is not based on consent from the data subject, and that in most cases personal data processed by MPS is subject to legislation other than the GDPR. The personal data sharing provided in the questionnaire responses is likely to represent only part of the actual sharing taking place within the GLA. As part of GDPR readiness activities, the GLA may wish to prepare a more comprehensive data map and register of controls.

All functional areas operate at least basic data protection controls, including issuing a data protection policy, assigning responsibility for data protection to a data protection officer, and ensuring that employees are provided with face to face training, paper training or e-learning when they commence employment. The GLA and the functional areas should plan for GDPR training, and should consider delivering training at least annually. GLA may benefit from sourcing training centrally to service all functional areas.

GLA has an opportunity to seek out examples of good practice within the functional areas and look to replicate or centralise these examples where possible, perhaps in the first instance through a data protection committee that can facilitate sharing of information between data protection officers.

Introduction

The GDPR requires that personal data is:

- *Processed lawfully, fairly and in a transparent manner;*
- *Collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes ('purpose limitation');*
- *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- *Accurate and, where necessary, kept up to date;*
- *Kept in a form which permits identification of the data subject for no longer than necessary for the purposes for which the personal data are processed;*
- *Processed in a manner that ensures appropriate security of the personal data.*

Given the potential complexity of personal data sharing within the GLA, the review sought to establish the purposes of processing personal data and how and why it is shared with third parties.

Using Personal Data

The functional areas of the GLA use personal data for a wide range of purposes which reflect the diversity of the various bodies concerned *(Q1)*. Purposes of processing include (but are not limited to):

- **Service delivery:** Primary services include dispatching emergency response, running youth intervention programmes, enforcing fire safety regulations, recording and reporting casualties at emergency incidents, planning services, operating public wifi, property and leasehold management;
- **Intelligence:** Safeguarding venerable adults and children, identifying those most at risk from fire and providing interventions, strategic planning;

- **Employment:** Recruitment, pre-employment screening, employment, training, provision of staff services, health, disciplinary matters, volunteering, workforce efficiency and monitoring, post-employment, pensions administration;
- **Finance:** payments, revenue collection, reporting and audit;
- **Legal obligations:** Preventing, monitoring and recording health and safety incidents;
- **Promotion:** Running surveys, consultations and community outreach, events delivery;
- **Safety:** Prevention, detection and investigation of crime, licensing and regulation.

Data Protection Controls

The functional areas have key data protection controls in place (Q2), as shown in ***Table 1***.

CONTROL	GLA	LFEPA	LLDC	MOPAC	MPS	OPDC	TfL
Data protection policy	✓	✓	✓	✓	✓	✓	✓
Data protection procedures	✓	✓	✓	✓	✓		✓
Designated data protection officer	✓	✓	✓	✓	✓		✓
Data protection training and awareness	✓	✓	✓	✓	✓	✓	✓
System privacy specification/testing	✓	✓			✓	✓	✓
Internal or external audit	✓	✓			✓		✓

Table 1: Data protection controls

Note that whilst LLDC reports no use of internal or external audit for data protection, the organisation has been subject to two information security audits in the past 15 months.

Data protection policies are communicated to service users through a range of channels (Q3) as shown in ***Table 2***.

CONTROL	GLA	LFEPA	LLDC	MOPAC	MPS	OPDC	TfL
Contracts of employment	✓	✓	✓	✓	✓		
Intranet or collaboration spaces	✓	✓	✓	✓	✓	✓	✓
Training and awareness	✓	✓	✓	✓	✓		✓
Data protection 'champions'	✓			✓			✓
Internal emails or documents	✓		✓	✓	✓		✓

Table 2: Data protection controls

The functional areas confirm use of communications including face to face training, provision of data protection leaflets, embedding messages in other training courses, providing posters and newsletter articles, emails, intranet materials, log on 'splash screens', and inserts in induction packs.

Staff are trained in their data protection duties through a range of delivery channels *(Q4)* as shown in ***Table 3***.

CONTROL	GLA	LFEPA	LLDC	MOPAC	MPS	OPDC	TfL
Face to face training	✓		✓	✓		✓	✓
e-Learning	✓	✓			✓		✓
Paper-based training				✓			

Is training compulsory?	✓	✓	✓		✓		✓
Is training repeated regularly?		✓	✓	✓			✓
Is a record kept of training?	✓	✓	✓	✓	✓		✓

Table 3: Data protection controls

The provision of staff training is generally good, with all new starters subject to either face to face training, e-learning or paper-based training, and records are kept to evidence completion of that training. For example, all new staff joining the GLA are required to attend the Information Governance Induction Workshop training session, which provides an overview and introduction to freedom of information and data protection, as well as other information management and information security issues.

Of greater concern is the requirement to repeat training on a regular basis. This is being catalysed by the introduction of the GDPR, and over the coming year staff will need to be trained in new responsibilities, systems and processes arising from the GDPR.

Functional areas should plan for GDPR training, and should consider delivering training at least annually. GLA may benefit from sourcing training centrally to service all functional areas.

Sharing Personal Data

The functional areas were asked to provide information about the nature and purpose of personal data sharing within and outside of the GLA *(Q8, Q9).* The information received represents only a small part of the likely personal data sharing that takes place, but even at this level is indicative of the complexity of personal data sharing within and outside of the GLA.

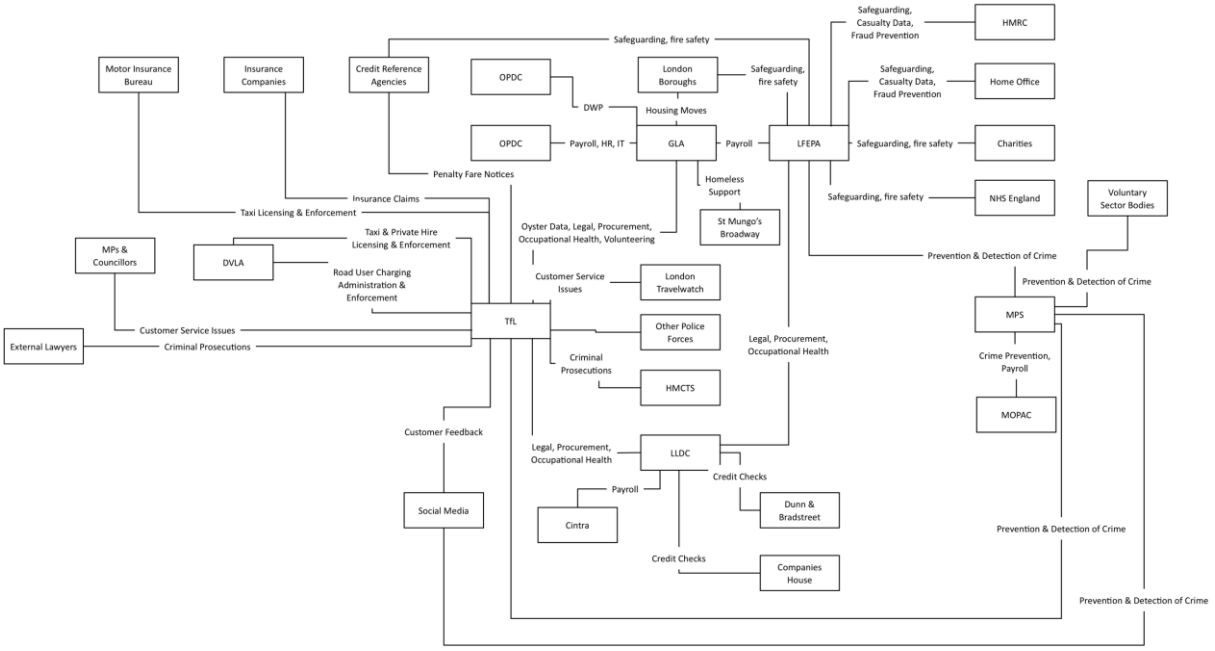

Figure: Sharing Personal Data

Functional areas commented on the complexity of personal data sharing and the need for simpler mechanisms to do so, and suggested the need to improve understanding of data sharing agreements so that they are used properly, and continuing to seek improved means for data sharing between public bodies where there is a clear public interest to do so.[1]

[1] https://data.blog.gov.uk/category/making-better-use-of-data/

Achieving a Standard of Good Practice for Data Protection

There is an indicated desire to examine 'good practice' for data protection management. However, the concept of good practice remains undefined within the profession, and encompasses a number of different possibilities which can be considered as follows:

- **Compliant:** Data protection practices that comply with the applicable legal and regulatory requirements;
- **Mature:** Data protection practices which are efficient, optimised and replicable;
- **'Privacy Positive':** Data protection practices which are structured around the data subject's needs and which prioritise data subject wishes over the organisation's needs.

There are no commonly-recognised international standards for data protection practice, and very few applicable certification schemes available (a notable exception is the US-based Truste scheme, which is largely aimed at US corporates wishing to demonstrate good practice in the handling of personal data on websites). Where standards exist, they are not necessarily of value for GLA functional bodies:

The UK's British Standards Institute has published BS10012 Specification for a Personal Information Management System, which will be revised shortly to reflect the GDPR, but has not received widespread adoption and is largely unknown in the data protection community;

The Canadian Institute of Chartered Accountants' interpretation of the Generally Accepted Privacy Principles to create a Capability Maturity Model provides a generic privacy maturity assessment which is valuable for understanding efficiency of privacy practices, but is not aligned with the GDPR;

The UK Information Commissioner's Office has published a range of codes of practice and guidelines for data protection, but these do not cover all areas of data protection and some need to be updated for the GDPR.

In general, it would be advisable for GLA to seek out examples of good practice within the functional areas and look to replicate or centralise these examples where possible, perhaps in the first instance through a data protection committee that can facilitate sharing of information between data protection officers.

Information Rights

Conclusions

Data protection laws require that controllers uphold information rights, and the GDPR will introduce new rights and new obligations upon controllers, regardless of the legal basis used for processing, which in many cases for GLA functional areas is a basis other than consent. It should be noted that for MPS in particular, even where methods other than consent are use, information rights principles apply and must be enforced (subject to legislative exemptions relating to prevention and detection and crime).

Where consent is required, the functional areas obtain consent and maintain a record of the consent obtained, as required by the GDPR. Nevertheless, the GLA should seek assurance that all functional areas have checked that where they use consent as a legal basis for processing, they have obtained and maintained a record of consent.

Despite the introduction of new information rights and the abolition of fees for subject access requests, the functional areas do not anticipate a rise in the volume or complexity of subject access requests (the majority of which are linked to employment disputes). The GLA may wish to maintain a watching brief on this situation, since a failure to uphold information rights will have significantly greater adverse consequences under the GDPR.

Requirement

Article 6 of the General Data Protection Regulation defines Lawfulness of processing as requiring at least one of the following conditions:

"…a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child…"

In many instances consent will not be the legal basis for processing, for example MPS may process for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or TfL may process for the performance of a contract to which the data subject is party. It would be reasonable to expect that most processing by functional areas, other than for providing news and information to the public and volunteers, would be under a legal basis other than consent.

Obtaining and Recording Consent

Article 7 of the GDPR requires that:

"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

This is a significant requirement for most data controllers, since it means that they must have a record of consent not only for new personal data, but for existing records which may have been collected long before this requirement. Furthermore, that consent must be obtained through an affirmative action on the part of the data subject: in most cases, this is likely to require fresh evidence of consent before May 2018, otherwise there may not be sufficient evidence of consent to continue processing.

Where consent is the legal basis for processing, the functional areas all ask individuals to opt in at the time of data collection *(Q10)*. TfL acknowledged that the organisation is still moving towards an opt-in only approach to the processing of personal data for promotional or marketing messages. This will need to be complete by May 2018.

The GLA should seek assurance that all functional areas have checked that where they use consent as a legal basis for processing, they have obtained and maintained a record of consent.

Four of the functional areas (GLA, LLDC, MOPAC and TfL) confirmed that they have a comprehensive record of consent provided *(Q11)*. LFEPA acknowledged that whilst consents are recorded, these are in separate systems and files, and that evidence of consent is not held in a single database. MPS does not rely on consent for the majority of its processing of personal data.

The functional areas were asked how individuals can access and manage their own personal data, including opting out of processing if they wish *(Q12).* Methods and channels are generally proportionate and effective, as shown in ***Table 4***.

QUESTION	GLA	LFEPA	LLDC	MOPAC	MPS	TfL
At time of collection regardless of channel	✓	✓	✓	✓		✓
Web contact form	✓	✓	✓			✓
Web self-service (i.e. online access to the data)	✓	✓	✓			✓
Post	✓	✓		✓		✓
Phone	✓	✓				✓
Email	✓	✓		✓		✓

Table 4: How can individuals access and manage their own personal data, including opting out of processing if they wish?

GLA and TfL confirmed that news emails include an unsubscribe link, and TfL operates a dedicated unsubscribe email address. LLDC already allows volunteers to manage contact preferences using an online account.

Information Rights Management

Despite a general rise in public awareness of data protection and information rights, there is no evidence from the questionnaire *(Q13)* to indicate a rise in the number of subject access requests received from members of the public over the past five years.

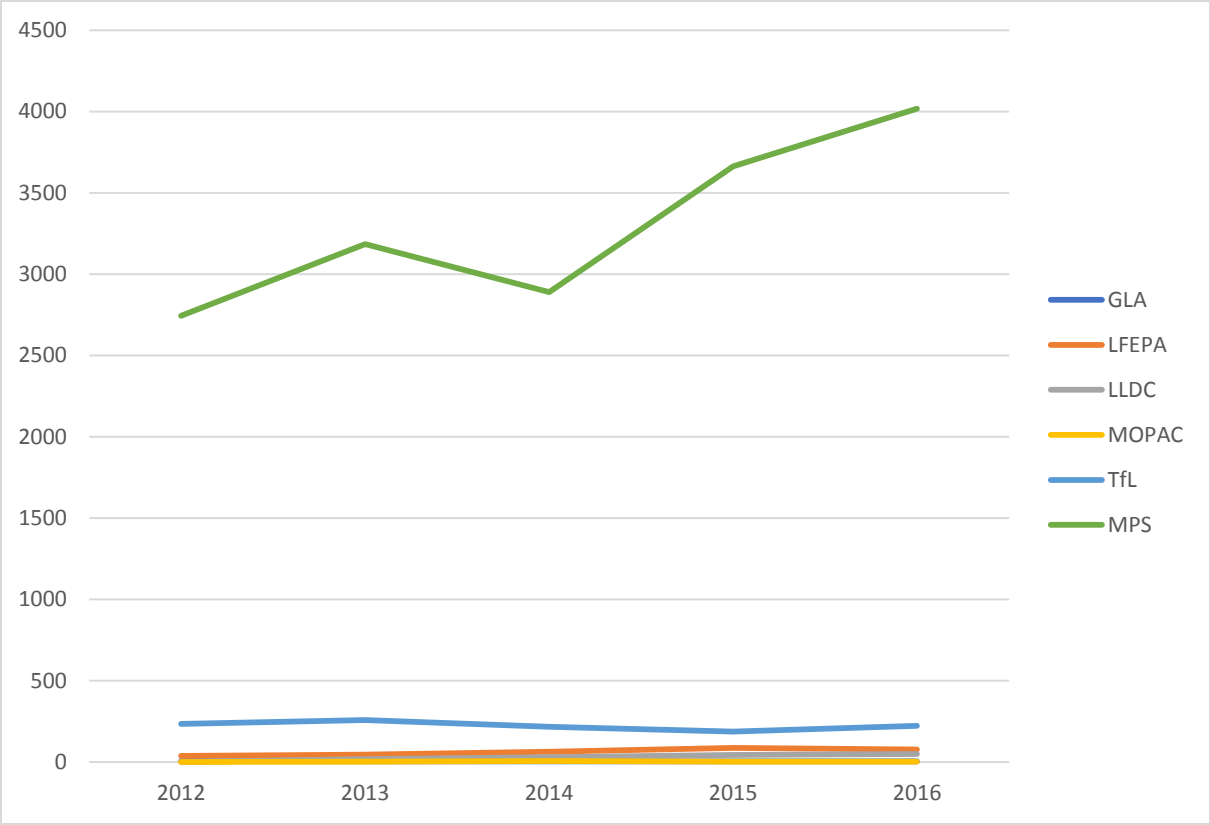

Figure: Subject Access Requests

Both GLA and LFEPA commented that most subject access requests come from current or former members of staff, and are linked to grievances, disciplinary matters or employment disputes (this is a common theme for most large employers in both public and private sectors). MPS' relatively high number of subject access requests will in part arise from their use in the legal process, and as such should not necessarily be interpreted as indicative of an underlying issue – indeed, MPS anticipates that the number of subject access requests will reduce in 2017 since the recent rise was in part due to requests from retired officers.

However, four of the six functional areas anticipate processing more subject access requests in future. This is likely to be influenced by the removal of the ability to charge for a subject access request under the GDPR (current requests are subject to a £10 fee).

Information Security

Conclusions

Each of the GLA's functional areas applies government standards or equivalent standards for the security of personal data, and as assigned responsibility for information security. Whilst information security breaches are inevitable, these appear to have been handled appropriately, and there is no evidence to suggest a systemic failure leading to an upward trend in information security incidents.

However the GDPR introduces new requirements for information security, and the GLA should monitor data protection resource requirements across the functional areas and ensure that adequate resources are assigned to ensure compliance with, and maintenance of, the demands of the GDPR. The GLA should also ensure that all functional areas implement mandatory GDPR controls, including the use of data protection impact assessments and the adoption of data protection by design and by default.

Given that the GDPR creates increased reporting requirements the GLA may wish to ensure that common standards are applied for breach reporting across all functional areas.

Requirement

The GDPR requires that personal data must be:

"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."

Responsibility for Information Security

Each of the functional areas has an assigned individual and/or team responsible for information security *(Q5)*. The GLA, LFEPA and MPS confirm that they have a Senior Information Risk Owner, and TfL has a Chief Information Security Officer who leads the Cyber Security and Incident Response Team. In the case of OPDC, information security is a shared service with GLA Governance.

Data Protection Risks

The functional areas were asked to comment on what they perceive as the main risks arising from the processing of personal data *(Q1)*. Their responses identify potential risk areas that include:

- Collection of excessive/unnecessary personal data (i.e. cannot be justified for a legitimate reason);
- Use of personal data for purposes not originally specified at the time of collection;
- Unauthorised access to, or use of, personal data;
- Loss, disclosure or corruption of personal data;
- Inappropriate or unauthorised sharing of personal data;
- Retention of personal data for longer than necessary for the specified purpose;
- Failure to uphold data protection principles or information rights.

The responses acknowledge that these risks can arise not solely through malicious causes, but from human error, for example emailing personal data to the wrong individual. One functional area cited a very real problem, that of legacy systems that do not support current information management policies and security objectives. This is a common cause of data protection failures in both public authorities and private companies.

Consequences of these risks were identified as

- Regulatory enforcement action by the Information Commissioner's Office (ICO) as a result of non-compliance with data protection legislation;
- Litigation by data subjects as a result of non-compliance with data protection legislation or a common law duty of confidence.

An additional risk not cited in the responses would be that of an enforcement action from a supervisory authority, i.e. forcing a suspension of processing until such a time as a problem can be remedied, which could have a very significant impact on the running of a public authority.

Security Standards

LFEPA, MOPAC and MPS apply the Government Security Policy Framework[2] as their standard for information security operations *(Q5)*. TfL and GLA (and therefore OPDC) apply their own proportionate security standards to personal data, but TfL applies the Security Policy Framework to information received by partner organisations such as government and law enforcement.

Controls used by the function areas include:

- Data minimisation (only obtaining and processing the minimum amount of personal data necessary for the specified purpose);
- Destruction of personal data once it is no longer required;
- Using personal data sharing and processing agreements;
- Maintaining a corporate risk register;
- Maintaining a personal data asset register;
- Incorporating privacy by design recommendations into system and project developments;
- Using data protection impact assessments to ensure that controls are appropriate to privacy risk.

These controls are claimed to be in place in the GLA, which may wish to ensure that they are replicated across the functional areas as part of readiness preparations for the GDPR.

Monitoring and Reporting Personal Data Incidents

With the exception of LLDC and OPDC, all of the functional areas have reported personal data incidents *(Q7)* to the Information Commissioner's Office (ICO), in accordance with the ICO's guidance on data security breach management.[3] In none did the ICO take further action regarding the breach.

[2] https://www.gov.uk/government/publications/security-policy-framework

[3] https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

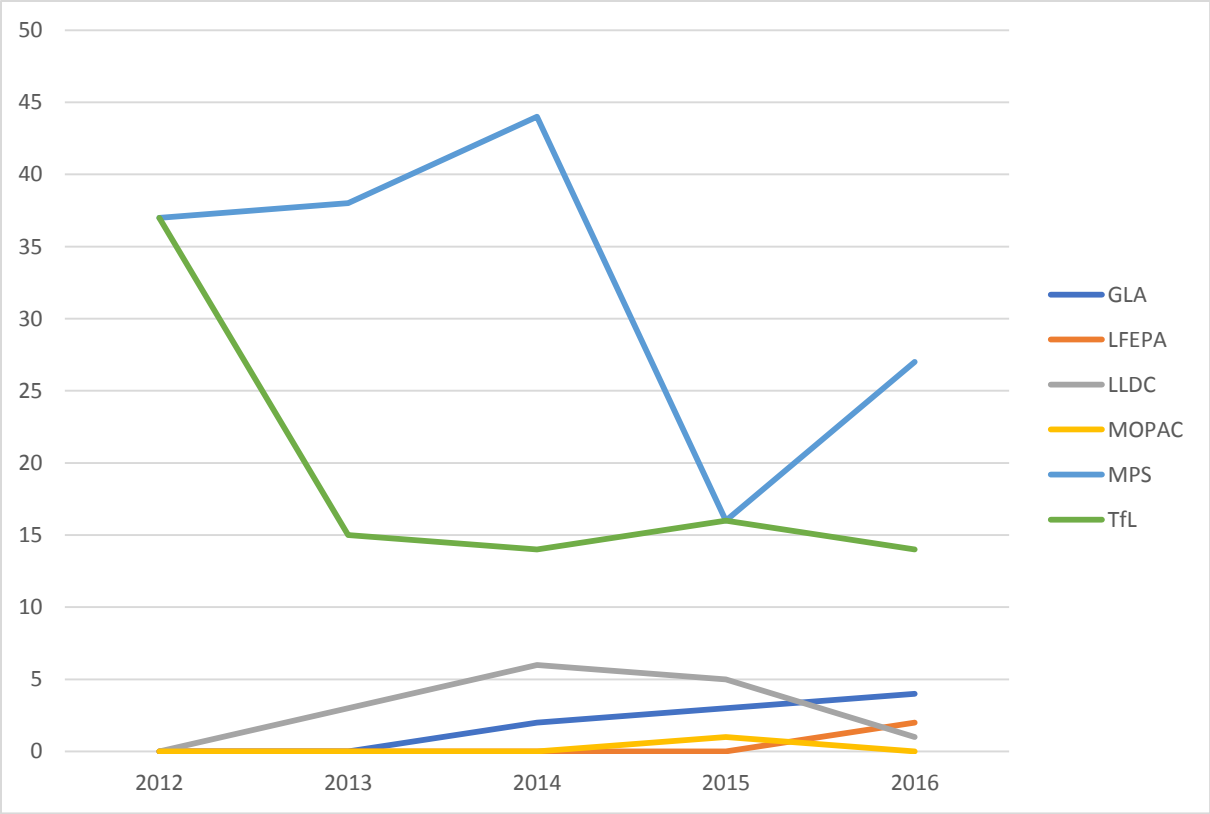

Figure: Personal data incidents by year

Where further information about the breaches was provided by the functional areas, the processes followed appear to be rigorous and transparent, and reflect good practice for breach management. The majority of breaches related to human error, in particular emailing personal data or copying in lists of individuals and thereby exposing personal details. TfL reported incidents involving criminal misuse of personal data by authorised individuals or former employees.

Personal Data Incidents

In keeping with legal obligations (notably the requirements of the Privacy & Electronic Communications Regulation (PECR) and the Information Commissioner's guidance on data breach management) the functional areas investigate data protection incidents and notify the Information Commissioner's Office where these are considered to pose a serious risk to the rights and freedoms of individuals.

Over the past five years, the functional areas have identified 285 data protection incidents, resulting in 10 notifications to the Information Commissioner's Office. Functional areas volunteered information about three complaints to the Information Commissioner not related to these incidents. Four of these incidents resulted in criminal investigations, but in no case were any of the functional areas penalised for reporting the incidents.

It should be noted that the incident notification procedures managed by GLA and TfL can be considered robust and effective (other functional areas may have similarly effective procedures but these were not included within the scope of review).

Given that the GDPR creates increased reporting requirements (although functional areas do not all see these as creating a greater volume of breach reports) the GLA may wish to ensure that common standards are applied for breach reporting across all functional areas.

Data Protection Risks

The functional areas were asked to comment on their concerns about personal data processing *(Q17)*. LFEPA raised their concerns that the increased burden on controllers arising from the GDPR may stretch limited data protection governance resources, and that when coupled with the increased regulatory powers and potential administrative fines, their organisations may require additional resources to keep pace with the anticipated changes over the coming years.

The GLA should monitor data protection resource requirements across the functional areas and ensure that adequate resources are assigned to ensure compliance with, and maintenance of, the demands of the GDPR.

GLA's team raised a related concern about the risk of projects and changes going ahead without taking into account the implications of handling personal data, and the need for data protection controls mandated by the GDPR, particularly through the requirement for data protection by design and by default, despite the guidance and advice published by the Information Governance team. The LFEPA team is improving engagement with projects to ensure compliance with data protection laws, including the provision of privacy by design recommendations, and the use of privacy impact assessments.

The GLA should ensure that all functional areas implement mandatory GDPR controls, including the use of data protection impact assessments and the adoption of data protection by design and by default.

The Future of Personal Data

Conclusions

The GLA and its functional areas are subject to a number of data protection laws, but the introduction of the GDPR will be the most significant change in those laws in decades, and it is imperative that preparations are in place. GLA functional areas believe that they will be prepared for the GDPR by the time of its enforcement in May 2018, but the GLA should nevertheless consider a root and branch review of readiness for the GDPR, with central coordination and monitoring of readiness plans, and prepare contingency plans to mitigate areas where the GDPR's requirements might not be implemented by May 2018. It should be noted that the GDPR is not the primary applicable legislation for MPS' processing of personal data, much of which is subject to the EU Law Enforcement Directive in place of the GDPR.

The UK's decision to leave the EU will not affect the applicability of the GDPR, and may introduce additional complexity for data protection management. The GLA has a role to provide central guidance on this for functional areas, and to prepare contingency arrangements should the UK's post-Brexit data protection environment not be considered to be equivalent to that of the GDPR.

Whilst there is agreement that data protection is likely to become more complex over the next five years, there was no sense from the questionnaire responses that the functional areas may need to make fundamental changes to the way that data protection is managed in the GLA.

The General Data Protection Regulation

The General Data Protection Regulation (2016/679) (GDPR) is the most significant overhaul of data protection legislation since the introduction of the original Data Protection Directive in 1995. It was enacted in 2016 and will be enforceable from 25th May 2018, and applies to private sector organisations and public bodies alike. Whilst the GDPR is built upon the data protection principles and information rights established under the Data Protection Directive, it creates significant new rights for individuals, responsibilities for controllers, and rights for individuals, as summarised below:

NEW RIGHTS FOR INDIVIDUALS

- Extraterritorial protection for EU residents regardless of where or by whom their personal data is processed;
- Rights to access, rectification, erasure, restriction of processing, notification, data portability, object to processing, opt out of profiling or automated decision making;
- Right to complain to a supervisory authority about processing;
- Right to representation by a third party (e.g. a consumer body, class action group or claims company);
- Right to compensation and liability (i.e. right to sue for damage or distress).

NEW RESPONSIBILITIES FOR CONTROLLERS

- Requirements for data protection by design and by default in the design and delivery of systems;
- Responsible for actions of processors who might process personal data on the controller's behalf;
- Designate a data protection officer to manage data protection and represent individuals' interests;
- Complete data protection impact assessments on projects and changes which might affect the rights or freedoms of individuals;

- Duty to notify supervisory authorities of breaches, and to communicate breach details to affected data subjects.

NEW POWERS FOR SUPERVISORY AUTHORITIES

- Ability to enforce restrictions of processing and to impose substantial administrative fines for failure to implement controls or for mishandling of personal data.

GLA functional areas were asked to comment on the anticipated impact of the GDPR and their readiness for its implementation *(Q14)*.

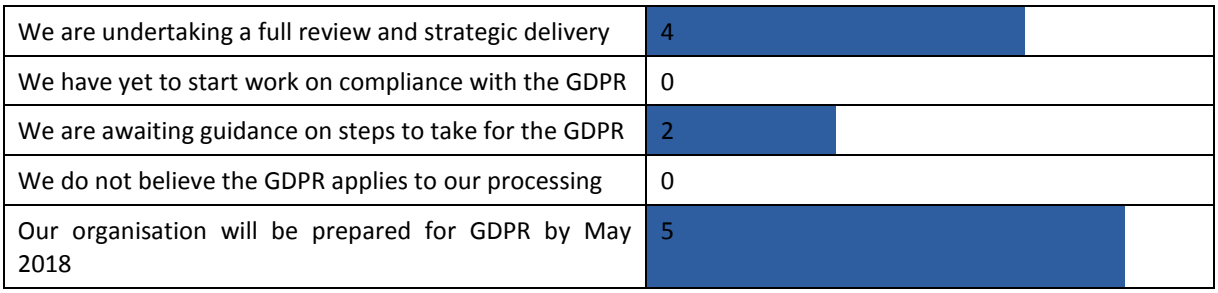

Figure: Preparing for the GDPR

All functional areas anticipate being prepared for the GDPR by May 2018. The GLA has recently started work on preparing for the introduction of the GDPR by conducting a review of the personal data asset register, and will be working on a delivery plan to identify how the new elements of the GDPR will affect existing processes, procedures, data assets, privacy/fair-collection notices and contractual and data process/sharing arrangements. The delivery plan will also look to ensure the GDPR is incorporated into the delivery schedules for existing projects, proposals, schemes and agreements, such as formally incorporating Privacy by Design recommendations and Privacy Impact Assessments into GLA workflows and governance frameworks.

TfL acknowledges that a significant programme of work is required to prepare for the implementation of the GDPR. Some of that work is already underway, for example the review and revision of privacy notices; information sharing agreements; and data processor contract terms and conditions.

Nevertheless, the GLA should not underestimate the work required to prepare for the GDPR, and the potential consequences of failure to prepare.

The GLA should initiate a root and branch review of readiness for the GDPR, with central coordination and monitoring of readiness plans, and prepare contingency plans to mitigate areas where the GDPR's requirements might not be implemented by May 2018.

Brexit

The UK's decision to leave the European Union, which is anticipated to happen in 2019, will end the applicability of the GDPR for UK processing personal data about UK residents. However, it is generally expected that in practice the requirements of the GDPR will continue to apply to all UK organisations, since:

- The GDPR will be the applicable data protection legislation from 25th May 2018 until such a time as the UK leaves the EU;
- The GDPR will continue to apply to personal data about EU residents processed by UK organisations (an 'extra-territorial' quality of the legislation);

- The government and the Information Commissioner have stated[4] their intention to align subsequent UK data protection legislation with the GDPR so that the UK can obtain an opinion of 'adequacy' from the European Data Protection Supervisor, which will allow UK organisations to exchange personal data freely with EU Member States without the need for additional legal safeguards.

The functional areas generally believe that Brexit will not affect the management of personal data in their organisations *(Q16)*, since they are aware of the government's position on the implementation of the GDPR. TfL raised a note of caution, saying *"it is unclear how [the UK] intends to modify or maintain that legislative framework after the UK leaves the EU. For example, if any changes are made to the GDPR after the UK has left the EU, will the UK choose to amend domestic legislation to maintain consistency with its EU trading partners."*

The GLA should continue to monitor the implications of Brexit, and in particular:

- ***Provide support to the functional areas should there be legislative changes requiring changes in the controls and capabilities across the functional areas;***
- ***Consider the potential implications for the functional areas, their partners and suppliers, should the UK not manage to obtain an opinion of adequacy from the European Data Protection Supervisor, thereby complicating the legal safeguards required to exchange data with EU Member States or to process personal data relating to EU residents.***

In addition to the GDPR, a related Data Protection Directive is intended to align the use of personal data for the prevention and investigation of crime. Whilst this is likely to impact GLA functional areas, and in particular MPS, it is not within the scope of this review and will not apply until such a time as the UK government implements national legislation to deliver the requirements of the Directive.

Future Developments in Data Protection

The functional areas were asked to comment on anticipated changes in their personal data handling over the next five years *(Q15)*.

QUESTION	MORE	SAME	LESS
The amount of personal data we will process	4	2	
The sensitivity of personal data we will process	2	4	
The amount of personal data we share with or obtain from government bodies	3	3	
The amount of personal data we share with or obtain from private-sector companies	3	3	
The cost of managing data protection	4	2	
The amount of control we give individuals over their personal data	4	2	

Figure: How might your organisation's collection and use of personal data change over the next five years?

The majority of functional areas (including those processing the bulk of personal data) believe that the amount and sensitivity of personal data processed is likely to rise over the next five years, and with it the cost of managing data protection is likely to increase. As the GLA response states:

"We anticipate an increase is likely given the changing nature of the Authority's engagement and increased interaction with the public. New schemes and programmes run by the GLA may result in the

[4] https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/

GLA processing more personal data. It is therefore also likely the GLA will engage with an increasing number of delivery partners or data processors to manage, share or process that personal data with, or on behalf of, the GLA."

The functional areas are engaged (or expect to engage) in various projects including housing regeneration, telehealth, smart parks and personalised travel that will increase the volume and sensitivity of personal data processed. Personal data sharing needs are anticipated to rise, and there is likely to be a commensurate rise in data protection controls and interfaces to enable individuals to express and manage their wishes for consent and information rights mandated by the GDPR.

Data Protection Opportunities

The functional areas were asked how they might benefit from changes to personal data processing in the future *(Q18)*. Whilst there were no shared themes for opportunities, suggestions included:

- The improvements to data protection policies and practices required by the GDPR will strengthen organisational awareness of handling personal data and ensure a renewed focus on individuals' rights, including promoting greater degrees of openness and transparency with the general public in the management and processing of personal data. This in turn might strengthen engagement with the public.
- The use of a Customer Relationship Management (CRM) based system to capture all 'person centric' data, including consent and preferences for handling personal data, could both facilitate compliance with the GDPR, and improve customer engagement.

Data Protection Improvements

Finally, the functional areas were asked what they might change about the way their organisations process personal data *(Q19)*. A theme raised by two functional areas was the management of data sets and information rights, with a proposal that a central register of personal data sets across the GLA group might improve efficiency, and if coupled with a a data protection management application, this could allow information governance teams to respond to information rights requests in a timely manner.

It was also suggested that the GLA should pursue a shift in perceptions so that data protection is seen not just as a compliance activity but rather as a vital – and positive – element of protecting individuals' rights, and an opportunity for the GLA to build trust.

Observations by Functional Area

Introduction

Each of the GLA functional areas under review returned a questionnaire response, which has been summarised below.

Greater London Authority (GLA)

In its role as a strategic delivery authority, the GLA processes relatively little personal data, but much of this is under consent as a legal basis for processing. The GLA tries to avoid joint-controller or controller-processor arrangements, which simplifies the data protection management process and reduces processing risks. Risk is tracked on the corporate risk register, and robust data protection controls are used to manage and mitigate risks, including appointment of a data protection officer, use of policies and procedures, awareness training, privacy by design requirements and compliance checks. The GLA's processing was audited in 2015/2016, and a follow-up audit is under way.

The GLA has a well-defined and comprehensive data protection management structure, which includes an incident management structure that notifies incidents to the Senior Information Risk Officer. Only nine incidents have been reported in the past three years, and of these only one required notification to the Information Commissioner's Office, but has not resulted in further action.

Personal data sharing is limited to the minimum necessary for specific projects, such as social development and homelessness. Where the GLA collects personal data from data subjects, it is subject to information rights management including privacy notices and consent statements. Data subjects can contact the Information Governance team to manage their data rights through web, post, phone or email channels. The GLA receives approximately three subject access requests each year, mainly related to employment issues.

The GLA is preparing for the GDPR, including reviewing the personal data asset register, implementing privacy by design recommendations and data protection impact assessment processes, and is confident in achieving compliance by May 2018.

London Fire and Emergency Planning Authority (LFEPA)

LFEPA makes extensive use of personal data, for purposes including employment, safeguarding, emergency response, enforcement of fire safety regulations, recording casualties and preventing and detecting crime. The organisation runs a dedicated information access team to support data protection requirements, and operates comprehensive security and data protection policies.

LFEPA has identified two personal data breaches over the past five years, and on each occasion has notified the Information Commissioner's Office with no further action taken. The team note that with increased reporting obligations under the GDPR, it is probable that the number of breaches reported will rise significantly.

LFEPA retain a record of consent obtained where that is the legal basis for processing, although consent records are not centralised into a single data store. Information rights management includes the option for data subjects to manage their data through an online interface, which supports the high volume of information rights cases handled by the team, which are mostly related to employment disputes. The LFEPA team anticipate a rise in the number of cases when the GDPR is enforced. LFEPA are reviewing GDPR requirements and anticipate being prepared by May 2018.

London Legacy Development Corporation (LLDC)

LLDC uses personal data for a range of purposes, including employment, operations, volunteering and provision of public wifi services in the Park. Personal data sharing is limited to payroll services and background checks for customers and suppliers.

LLDC applies information security controls which include data protection controls, covering policies, employee training, audits and employee awareness activities, and training was provided to over 270 employees last year. The organisation maintains a risk register and tracks data protection breaches, but of the 15 breaches in the past five years there has been no requirement to notify the Information Commissioner's Office because they mostly related to leaving personal data on printers, rather than a loss or misuse of personal data. LLDC has been the subject of two complaints to the Information Commissioner, one relating to the use of a cc: field in an email communication that identified 7 other individuals, and the other for an individual being accidentally subscribed to a newsletter without providing consent. No further action was taken by the Commissioner.

The LLDC team anticipate a rise in the amount, sensitivity and cost of personal data handling, linked to the growth of the organisation.

Mayor's Office for Policing and Crime (MOPAC)

The response from MOPAC makes clear that most of the use of personal data by MOPAC relates to the work of the Professional Standards team and pre-employment vetting of its own staff. The organisation operates a reasonably comprehensive data protection regime, and has suffered a single data protection breach in the past five years, which was notified to the Information Commissioner's Office.

Personal data sharing is confined to exchanges with MPS, and use of shared HR services provided by GLA. Where consent is the legal basis for processing, MOPAC obtains and maintains a record of that consent. MOPAC's management are awaiting guidance on how to prepare for the GDPR, but do not anticipate major changes in the way that the organisation processes personal data.

Metropolitan Police Service (MPS)

The majority of MPS' processing of personal data does not use consent as a legal basis, and instead relies on other legal bases including public safety, public interest, legal obligation and protecting the vital interests of individuals. Whilst the information rights described in the GDPR will still apply to personal data processing, other requirements come from the EU Law Enforcement Directive, which provides an enabling mechanisms for the sharing of personal data between law enforcement authorities. The Home Office has yet to provide guidance on implementation of the Directive, and in the meantime MPS is applying the Information Commissioner's GDPR guidance since the information rights management issues will remain broadly similar.

MPS processes personal data for the prevention and detection of crime, and operates a comprehensive data protection management structure, with designated risk owners responsible for policies, processes, training and delivery. The MPS tracks personal data breaches, and has notified the Information Commissioner of a breach that lead to no further action.

MPS' team are of the opinion that the amount of personal data processed will rise in future, as will the cost of managing data protection, and are concerned that a 'silo' approach to data management may give rise to data protection risks.

Oak Park Development Corporation (OPDC)

OPDC makes very little use of personal data beyond the contexts of employment and handling queries from the public. IT services are provided by GLA, and there is no sharing of personal data

with other bodies. The organisation has not been subject to information rights requests or complaints, and is not aware of any personal data breaches having taken place. Data protection management services are provided by GLA, and OPDC anticipates GDPR readiness being provided through those services.

Transport for London (TfL)

TfL is arguably the largest processor of personal data within the GLA functional areas. Uses of personal data and sharing of that data are extensive, as shown in ***Figure 1***. TfL has a professional information governance team responsible for managing data protection and information rights issues, and they deliver a comprehensive suite of controls including policy, procedures, training, testing and audits.

TfL operates a computer security incident response team that monitors and manages incidents, and has reported four incidents to the Information Commissioner's Office over the past five years. All four incidents have been resolved without action against TfL, and criminal action has been taken against the individuals concerned.

TfL's data sharing is extensive and detailed, with numerous public authorities and private companies providing and receiving personal data for different purposes, as shown in ***Figure 1***. TfL operates a template information sharing protocol, procedure and non-disclosure agreement to ensure consistent handling of data protection issues, and these are aligned with the Information Commissioner's Office's guidance.

Where consent is the legal basis for processing, TfL is migrating towards the 'opt in' approach mandated by the GDPR. The organisation anticipates significant further work needed to ensure GDPR readiness, including revisions to privacy notices, information sharing agreements and data processor contracts.

This move towards GDPR readiness should support increased personalisation of information services, which TfL recognises represent an opportunity both to improve customer services and operational efficiency.

Appendix A: Questionnaire

General		
1	Describe the key ways in which the use of personal data help your organisation meet its strategic aims and objectives, and what are the main risks involved?	
	Strategic aims and objectives	
	Risks	
2	How do you make sure your organisation complies with the Data Protection Act 1998? *(Mark all that apply and provide copies of your organisation's policies relevant to personal data)*	
	Data protection policy	
	Data protection procedures	
	Designated data protection officer or equivalent	
	Data protection training and awareness	
	System specifications / systems testing to confirm privacy compliance	
	Internal or external audit of personal data handling	
	Other	
3	How do you communicate these policies to service users? *(mark all that apply)*	
	Contracts of employment	
	Intranet or collaboration spaces	
	Training and awareness	
	Data protection 'champions' in departments, buildings or functions	
	Internal emails or documents	
	Comments	
4	What training do your staff undertake to help them comply with the Data Protection Act? *(mark all that apply)*	
	Face to face training	
	e-Learning	
	Paper-based training	
	Is training compulsory?	
	Is training repeated regularly (e.g. annually)?	
	Do you keep a record of training?	
Security		
5	Which individuals and functions at your organisation are responsible for information security?	
	Please describe	

	Does your organisation have a designated information security officer(s)? *(y/n)*	
	Does your organisation apply the requirements of the government Security Policy Framework?[5] *(y/n)*	
	Comments	
6	How do you monitor and report on personal data incidents? *Please send us the last relevant report your organisation has produced*	
7	How many personal data incidents are you aware your organisation has had in each of the last five years?	
	2016	
	2015	
	2014	
	2013	
	2012	
	Have you reported personal data incidents to the Information Commissioner's office? *(y/n)*	
	What was the outcome?	
	Comments	

Data use and sharing

8	Do you obtain personal data from other organisations? Please give examples of sources and purposes			
		Y/N	**Source**	**Purpose**
	Other GLA organisations			
	Other public bodies			
	Commercial data (e.g. credit reference)			
	Public domain data			
	Other			
9	Do you share personal data with any other organisations? If so, which organisations and for what purposes? *(mark all that apply)*			
		Y/N	**Destination**	**Purpose**
	Other GLA organisations			
	Other public bodies			
	Commercial (e.g. credit reference)			

[5] https://www.gov.uk/government/collections/government-security#security-policy-framework

	Public domain			
	Other			
	How do you ensure partner organisations store and use this data appropriately?			
	Comments			

Individual rights		
10	Where consent is the legal basis for processing, how is consent obtained from individuals for the collection and use of their personal data? *(mark all that apply)*	
	Individuals are asked to opt in at the time of collection	
	Individuals are given the opportunity to opt out at time of collection	
	Consent is assumed, but individuals may contact the organisation to opt out of processing	
	The organisation has yet to implement a consistent mechanism to manage consent	
	Other	
11	Where consent is the legal basis for processing, does your organisation retain a documented record of the consent provided? *(mark one only)*	
	Yes, we have a comprehensive record of consent provided	
	Sometimes, but the record of consent provided is incomplete/inaccurate	
	No, but we can infer consent from the source of the data	
	No, we do not record the consent provided	
	Comments	
12	How can individuals access and manage their own personal data, including opting out of processing if they wish? *(mark all that apply)*	
	At time of collection regardless of channel (online, post, phone)	
	Web contact form	
	Web self-service (i.e. online access to the data)	
	Post	
	Phone	
	Email	
	Comments	
13	Approximately how many subject access requests has your organisation received in each of the last five years?	
	2016	
	2015	
	2014	

	2013			
	2012			
	Do you anticipate processing more or fewer subject access requests in future?	**More**	**Same**	**Less**
	Comments			
Future developments				
14	What steps are you taking to prepare for the General Data Protection Regulation (GDPR) (2016/679) expected to come into force in 2018? *(mark one only)*			
	• We are undertaking a full review and strategic deliver			
	• We have yet to start work on compliance with the GDPR			
	• We are awaiting guidance on what steps to take for the GDPR			
	• We do not believe the GDPR applies to our processing			
	• Do you anticipate your organisation will be prepared for the GDPR by May 2018?	**Yes**	**No**	
	Comments			
15	How might your organisation's collection and use of personal data change over the next five years? *(mark all that apply)*			
		More	**Same**	**Less**
	• The amount of personal data we will process			
	• The sensitivity of personal data we will process			
	• The amount of personal data we share with or obtain from government bodies			
	• The amount of personal data we share with or obtain from private-sector companies			
	• The cost of managing data protection			
	• The amount of control we give individuals over their personal data			
	Comments			
Other issues				
16	How do you think that the UK's exit from the European Union will affect the management of personal data for your organisation? *(mark one only)*			
	• It should simplify data protection (e.g. GDPR might no longer apply)			
	• It will make data protection more complex (e.g. new or changed laws)			
	• It will make no difference to data protection			
	• Don't know			

	Comments
17	What is your greatest concern about the way your organisation processes personal data? *(please describe)*
	Comments
18	What opportunities do you think your organisation could benefit from through changes to personal data processing in the future? *(please describe)*
	Comments
19	If you could change one thing about the way your organisation manages personal data, what would it be? *(please describe)*
	Comments

Appendix B: Documents Provided

The following documents were provided to support questionnaire responses to the review.

Greater London Authority (GLA):

- Data Protection Breach Notification Form (December 2016)
- Data Protection Policy
- Details of personal data incident and supporting documents (December 2016)
- FoI Processes Guidance
- FoIA Guidance Note – Datasets & FoI
- Info Gov Induction DPA slides
- Letter from Gareth Bacon AM to Tom Middleton (23rd December 2016)
- Transparency of the GLA Group (June 2013)
- Transparency of the GLA Group and Family (February 2016)

London Fire and Emergency Planning Authority (LFEPA):

- Law Commission Data Sharing Consultation 2013

London Legacy Development Corporation (LLDC):

- Acceptable Use of IT v3.2
- Information Compliance Policy v2.2
- Information Governance Report 2015-16 v1.0
- Information Management Policy v2.2
- Contract of Employment- Permanent

TFL:

- An introduction to the General Data Protection Regulation (May 2016)
- Collection of WiFi tracking data by TfL
- Information and Records Management Policy
- Information Security Policy
- Letter from Mike Brown MVO to Gareth Bacon AM (23rd January 2017)
- Overarching Information Sharing Protocol Agreement
- Privacy and Data Protection Complaints Handling Procedure
- Privacy and Data Protection Compliance Programme (May 2016)
- Privacy and Data Protection Policy
- Privacy and DP Programme Summary (May 2016)
- Template - TfL Agreement for provision and use of confidential info