



LONDON FIRE BRIGADE

Decision title

## General Data Protection Regulation – Readiness

Recommendation by	Decision Number
Data Protection Officer (Head of Information Management)	LFC-0017-D

**NOT PROTECTIVELY MARKED**

### Summary

LFC-0017 updates the London Fire Commissioner on the progress of work to prepare for the implementation of the new data protection regime introduced by the EU's General Data Protection Regulation (GDPR) and the new Data Protection Bill/Act 2018. This report seeks to provide assurance to the Commissioner that the London Fire Brigade will be broadly compliant with the GDPR from 25 May 2018 (when the new arrangements come into effect).

The report describes the work undertaken by the ICT/Information Access Team to prepare departments for the changes, explains the new products delivered as part of this work, and details some of the (minor) issues discovered during the information audit that has been carried out.

### Decision

The London Fire Commissioner receives the report.

**Dany Cotton QFSM**  
London Fire Commissioner

Date **22-5-2018**

### Access to Information – Contact Officer

<b>Name</b>	<b>Steven Adams</b>
<b>Telephone</b>	0208 555 1200
<b>Email</b>	governance@london-fire.gov.uk



LONDON FIRE BRIGADE

Report title

---

## General Data Protection Regulation – readiness

---

Report to

Commissioner's Board

Date

9 May 2018

---

Report by

Data Protection Officer (Head of Information Management)

Report number

LFC-0017

---

### NO PROTECTIVE MARKING

---

#### Summary

This report updates the London Fire Commissioner and the Board on the progress of work to prepare for the implementation of the new data protection regime introduced by the EU's General Data Protection Regulation and the new Data Protection Bill/Act 2018. This report seeks to provide assurance to the Commissioner and the Board that the Brigade will be broadly compliant with the GDPR from 25 May 2018 (when the new arrangements come into effect).

The report describes the work undertaken by the ICT/Information Access Team to prepare departments for the changes, explains the new products delivered as part of this work, and details some of the (minor) issues discovered during the information audit that has been carried out.

#### Recommendation

The Commissioner's Board notes this report.

## Background

1. The former Corporate Management Board (CMB) in June 2017 (CMB045/17) was advised of the potential impact of the changes to the data protection regime that would be introduced by the EU's General Data Protection Regulation. The CMB received an update about the progress of preparations by virtue of the draft report submitted to the Board in October 2017 (CMB111/17) targeted for the former LFEPA Governance, Performance and Audit Committee (GPAC) in November 2017 (FEP2805).

## GDPR – evolution not revolution

2. It is worth saying at the outset that as part of an ICO online blog to 'bust' some of the myths that have developed around the GDPR, the ICO has said:

*"The new regime is an evolution in data protection, not a revolution... It demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. GDPR is building on foundations already in place for the last 20 years... If you are already complying with the terms of the Data Protection Act, and have an effective data governance programme in place, then you are already well on the way to being ready for GDPR... Many of the fundamentals remain the same and have been known about for a long time. Fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose data you want to process – these are all things you should already be doing with data and GDPR seeks only to build on those principles... That doesn't mean there's any room for complacency. There are new provisions to comply with... But by and large, the new GDPR regime represents a step change, rather than a leap into the unknown."*

3. Expressing her view in this way has been helpful confirmation of officer's views and the Brigade's approach to implementation and preparations.

## GDPR and the new Data Protection Bill

4. The GDPR is a Regulation, meaning that it will be directly applicable across the EU, without the need for any domestic implementing legislation. Importantly however, the GDPR leaves plenty of gaps for member states to fill in. For example, it is up to member states to stipulate the grounds on which 'special category' personal data (formerly known as 'sensitive personal data' in UK law) can be processed. Exemptions from some individual rights and obligations (such as the right to make a subject access request, the right to be forgotten and to have personal data rectified) are also matters for member states.
5. As outlined in the November GPAC report (FEP2805), the government published a new Data Protection Bill on 13 September 2017. One of the main functions of the Bill is to fill in the gaps in the GDPR.
6. Another of the Bill's functions is to extend the GDPR into areas of data processing where it would not otherwise reach. For example, the GDPR does not apply to law enforcement or intelligence services activity, but the Government has voluntarily imposed a GDPR-like regime in those areas.
7. A third function of the Bill is to attempt to make UK data protection law Brexit-proof. Once the UK leaves the EU, the GDPR will no longer be directly applicable. Crucially, however, a post-Brexit UK will need to have in place a data protection regime that mirrors the GDPR; otherwise, the transferring of personal data between the UK and the EU will be extremely problematic. The Bill therefore strives to make UK data protection law stand on its own two feet while tracking the GDPR.

8. However, the Bill does not simply transpose the guts of the GDPR into UK law, and is not a copy-and-paste of the GDPR. Instead, it constantly cross-refers to the GDPR, meaning that one has to read both the Bill and the GDPR side by side. Neither document alone gives the complete picture of data protection in the UK.
9. The Bill is expected to be law by 25 May 2018 when the GDPR takes effect, but there is no firm confirmation of this yet. There is nothing from the ICO to suggest that organisations should do anything other than expect its adoption by the GDPR go-live date.

### **Data Protection Officer**

10. As the Commissioner's Board will know, the GDPR (and the Data Protection Bill) requires public authorities to appoint a Data Protection Officer (DPO). The role of DPO can be allocated to an existing employee so long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interest.
11. The former Corporate Management Board agreed, in November 2017 (CMB111/17), that the Head of Information Management (HoIM) should be the Brigade's Data Protection Officer (DPO). The LFC formally approved this arrangement by adopting the LFC Scheme of Governance (LFC-0003) that identified the Head of Information Management as the DPO within the appointment of statutory and proper officers (Part 5).
12. The DPO's minimum tasks, as set out in the GDPR and the DP Bill are to:
  - Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
  - Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
  - Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers, etc.).
13. The job description for the HoIM is being updated to reflect the DPO responsibilities.

### **Data breaches**

14. The GDPR introduces a duty on all organisations to report personal data breach to the Information Commissioner (ICO) where the breach is likely to result in a risk to the rights and freedoms of the individual(s). Breaches reportable to the ICO must be made within 72 hours of becoming aware of the breach, where feasible.
15. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then individuals must also be informed without delay.
16. As is the arrangement now, any actual or suspected data breaches must be reported to the DPO (via the Information Access Team) who will investigate the breach and decide whether or not the ICO and the affected individuals need to be notified. Through the awareness work to raise the staff and manager understanding of data protection issues, we will continue to encourage staff to report all data breaches, even those of a minor nature.
17. The Greater London Authority (GLA) have developed a breach reporting assessment tool they have developed, based on NHS work, and we plan to use this to assess when data breaches should be reported to the ICO. A record of all notified data breaches and the outcomes from investigations will be recorded by the DPO.

## **Contracts for supplies/services**

18. The ICO published draft guidance on the GDPR and its impact on contracts on 13 September 2017 for a short consultation period which closed on 10 October; no final version of the guidance has yet been published. The draft guidance says:
- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
  - These contracts must now include certain specific terms, as a minimum.
  - These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
  - The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors – though none have been drafted so far.
  - The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
  - The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.
19. Since then, Crown Commercial Services published Procurement Policy Note 03/17 which set out an approach to GDPR for contracts under the CCS framework.
20. The Information Access Team have been working in tandem with General Counsel and the Assistant Director, Technical and Commercial, to agree a set of standard GDPR contract conditions, for use as variations to existing contracts and for use in new contract terms. This work has also been informed by the review of all contract clauses that has been undertaken for the LFB by Sharpe Pritchard LLP.
21. Procurement staff are now working towards a process for the mass update of all existing contracts that have end dates past the 25 May GDPR effective date using the newly agreed clauses.

## **Information audit**

22. Board members will recall that the principle means by which the GDPR preparatory work has been carried out was via an Information Audit that would look at the personal data collected, held and processed. The audit would also look at whether processes connected to personal data were GDPR compliant. Brigade departments were prioritised into two groups – as a first priority, those departments/teams which were known to collect, hold and process personal data, and as second priority, the remaining departments.
23. The Brigade have a good track record for handling and processing personal data under the 1998 Act and have approached GDPR from what is considered to be a strong position. This strong starting point has been confirmed during the 'readiness' audits with few areas for concern coming to light which have been addressed directly when encountered. There are, however, some recurring themes where data protection and/or how teams within the organisation process personal data that could be improved. These include:

- *Email as a records/document management tool*: Individuals using email as a records management tool and unnecessarily keeping personal data within their email folders: This is a widespread issue that will be addressed as part of a wider review of records management/electronic document storage.
- *Staff personal data*: This is about how teams and departments store personal data related to staff. There are examples of separate files being maintained, or documents being saved to SharePoint EDMS rather than to the e-PRF. There is a case for extending access to the e-PRF system, potentially adding in department specific areas, so that most of the information recorded for an individual employee can be stored within one system.
- *Access to personal contact details*: Some teams are maintaining their own records of details for staff they contact as there are inconsistencies around how StARS/e-PRF records are accessed to obtain this information.
- *Data retention*: The Brigade has a well-established records retention strategy (PN0879), but this has been less successfully applied to electronic record systems like SharePoint. This will also be addressed within the review of records management/electronic storage.
- *Staff contracts*: Staff contracts already contain specific data protection clauses and these will be updated for all new contracts. At this time it is unclear whether or not the existing DPA clause will adequately transition to the GDPR regime. I am still in discussion with General Counsel colleagues about whether or not there is a need for all staff to re-sign employment contracts to reflect the new GDPR arrangements. In the end this will be a matter for the Assistant Director, People Services and General Counsel to resolve.

24. Other issues of a minor nature have been addressed with teams as they have arisen.

### **Information asset register/privacy notices**

25. As advised in previous reports, a key component of demonstrating that the Brigade's compliance with the GDPR is the creation and maintenance of an information asset register. The register records every type of personal data held, the legal condition for processing, how and why the data is processed, where it is stored and who has access (data security), where (if anywhere) the data is transferred and how and when the data is deleted (data retention).
26. A key part of the register is to codify the basis on which the LFC is processing personal data. This is deciding which of the 'legal processing conditions' the LFC will be relying on using one of the LFC's existing statutory powers, or the specific powers provided by the GDPR and/or the Bill. Very good progress has been made on identifying powers for most of the Brigade's personal data collection/processing. Some small issues remain with 'nailing down' the basis for some types of data processing, at the time of writing, although it is expected these will be resolved in the next few weeks.
27. There is considerable GDPR hype around using peoples personal data with 'consent' under GDPR. As advised in ICO guidance, the Brigade will only seek to use consent as a last resort and for the very few entirely voluntary activities (such as subscribing to the museum newsletter). In all other cases, the Brigade will be using other processing conditions such as the performance of a contract or undertaking a legal duty.
28. Through the practicality of this exercise, it emerged that the privacy notice could serve a dual purpose – being both the public facing explanation of how personal data is used, but also inform the information asset register. Beyond the 25 May 'deadline' officers will continue to work with to complete an information asset register (which is not required to be compliant with GDPR)

based on the data from privacy notices. The register will enable searches between the notices to see where similar data or processing conditions have been applied (for example, to produce a list of processes where special categories of personal data are used).

29. The team has adopted the ICO's approach to privacy notices whereby a layered system is recommended. This approach will mean that the information we need to provide to data subjects will be published at different levels of granularity depending on the circumstances or need. This layered approach will also avoid the need for staff to provide detailed multi-paged notices at the point of first contact. The first layer explains, at a very high level, how and why the Brigade need to process personal data and, most importantly, how an individual (data subject) can access more information or exercise their data protection rights.
30. Below this first level is a *General Privacy Notice* – setting out who the Brigade are, how to contact us and who the DPO is – and then individual *Data Processing Notice(s)* covering specific or related groups of processing activities. This is attached as an appendix to this paper.
31. The full hierarchy of notices will principally be available via the LFB website.

### **Policy updates**

32. The culmination of the preparation work will lead to a revised "Data protection and privacy" policy note (replacing policy 0351 (Data Protection Act 1998)). This will set out the Brigade's approach to data protection as well as containing the information that needs to be statutorily recorded under the GDPR and the text of the first level 'General Privacy Notice'. It will also deal with breach reporting (as outlined above). The policy will be supported by awareness and communications (see below).

### **Working with partners**

33. A series of meetings have taken place with other GLA group bodies to share experiences with GDPR preparatory work. These meetings have been useful in sharing common issues and concerns, understanding and learning. The data breach assessment tool, mentioned above, has been a tangible result of this joint working. Interestingly, some GLA group bodies that currently receive very few subject access requests (SARs) under the DPA, are expecting an increase in SARs because of the wide publicity about the implementation of the GDPR.
34. The Brigade is also working with the wider fire and rescue service on GDPR preparations, and was represented at a national GDPR conference on 1 November 2017 organised under the auspices of the National Fire Chiefs Council (NFCC). A significant volume of sharing/learning has been achieved via the online NFCC Information Governance forum (established as part of CFOA Communities and now being migrated to the NFCC Workplace Information Governance Group).

### **Staff training and awareness**

35. The focus of the preparatory work has been in the 'accountability and governance' requirements of GDPR, as set out in this report, working with senior staff and team leaders across departments. The Information Access Team fully understand the need for much wider communications to all Brigade staff and this is being put in place once we are satisfied that all the compliance obligations are met. This does mean that most of the wider communications will happen around, or soon after, the 25 May date.
36. An internal communication plan is being developed, in conjunction with the Assistant Director, Communications, that will set out a programme of awareness and communication initiatives, so that staff are fully aware of the GDPR and new Data Protection Act (when law) and the changes that need to be made in the processing and handling of personal data. Staff from the Information

Access Team, together with staff of the General Counsel's Department, continue to present to and brief teams and groups to raise the awareness of the GDPR requirements.

37. It will also be necessary to update, or replace, the current computer-based online awareness package (Cardinus software) which the Brigade uses to ensure and log basic data protection awareness for each member of staff. It is not possible to update the Cardinus system at this time as there are still some unknowns, in terms of the repeal of the current Data Protection Act, Royal Assent to the new Data Protection Bill and the confirmation of ICO guidance. However, the principles of data protection introduced by the GDPR are very similar to those of the Data Protection Act 1998, and because of this, the existing online training will be sufficient to provide staff with a basic understanding of their duties in relation to personal data, until it can be updated. As set out above, direct face-to-face inputs are appropriate in areas where staff regularly process personal data (e.g. in the People Services Department)
38. During the information audit, it was clear that all of the teams/individuals spoken to had a good understanding of what data protection meant and the high level steps that must be taken to protect personal data. Beyond the information access team, the knowledge of detailed data protection practices is less well understood. To comply with the GDPR it will be necessary to provide more bespoke training for those teams that process personal data as a significant part of their role. To get the most value from this training, I am of the view that it is best to look to do this some six to nine months after GDPR implementation so that some of the current uncertainties can bed down (including a final version of the Bill being enacted).

## Conclusions

39. The Brigade has a proven track record of complying with data protection principles and keeping personal data safe. On this basis, and having regard to all the preparatory work undertaken (as described in this paper), I am able to advise the Board that the Brigade will be compliant with the GDPR when it comes into effect on 25 May 2018. That is not to say that there will not be areas for improvement (as is the case now under DPA), but compliance has always acknowledged that organisation would seek to continuously improve.
40. At the changeover to GDPR all the key governance changes will be in place (using the ICO's 'steps to take' guide), the Brigade will have:
  - Ensured that key decisions makers and other key people in the Brigade are aware of the law changes.
  - Compiled an information asset register which sets out the personal data we collect, process and hold.
  - New privacy notices available on the Brigade's website which explain about the personal data we collect and process, the legal basis for collection and the data subjects' information rights.
  - Checked that our procedures, via the information audit, ensure they cover all the data protection rights individuals have.
  - Implemented arrangements to deal with request for personal data (subject access requests) within one month (instead of 40 days currently).
  - Documented the lawful basis for data processing under GDPR. This includes how we would seek, record and manage any data collection relying on consent.
  - Arrangement to report data breaches and reminded staff about the need to report any data breach to the Data Protection Officer.
  - Embedded the use of a privacy impact assessment for all new projects and activities that have an impact on personal data, to ensure we are operating on a 'privacy by design' basis.



- Appointed a Data Protection Officer.

41. The issues that will continue past the 25 May include:

- Updated contracts with suppliers to include new GDPR clauses in contract conditions (end July 2018).
- DPO and IA team to complete training for the Data Protection Practitioners qualification (end 2018)
- Online staff awareness training package to be updated/replaced (August 2018)
- Training material to be sourced for those staff that process significant amounts of personal data/sensitive personal data (Nov 2018)
- Review of the Brigade's approach to email retention (linked to Office 365/SharePoint Online) (March 2019)
- Review and revise the Brigade's approach to compliance in the light of actions by the ICO post 25 May.

42. To provide further reassurance, it is worth repeating (extracts) from a further post from the Information Commissioner's myth busting GDPR blog, where she draws a comparison with the Y2K preparations:

*"Unlike planning for the Y2K deadline, GDPR preparation doesn't end on 25 May 2018 – it requires ongoing effort... It's an evolutionary process for organisations – 25 May is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.*

*I want to reassure those that have GDPR preparations in train that there's no need for a Y2K level of fear... That said, there will be no 'grace' period – there has been two years to prepare and we will be regulating from this date.*

*But we pride ourselves on being a fair and proportionate regulator and this will continue under the GDPR ... Those who self-report, who engage with us to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider any regulatory action.*

*Yes budgets can be tight, technology is moving fast and there's a race to keep up with competitors. But if you can demonstrate that you have the appropriate systems and thinking in place you will find the ICO to be a proactive and pragmatic regulator aware of business needs and the real world."*

### **Finance comments**

43. This report provides an update on the progress of work to prepare for the implementation of the GDPR. The report notes that it will be necessary to provide bespoke training for some teams, nine to 12 months after the introduction of GDPR. Any financial implications of this should be considered as part of the budget process for 2019/20.

### **Workforce comments**

44. No consultation with the staff-side has taken place on this report. The Unison representative on the Joint Committee for Support Staff (JCSS) has recently (end April) asked about the Brigade's preparations for GDPR and I have provided him with information.

### **Legal comments**

45. General Counsel has reviewed this report and has no comments.

### **Sustainability implications**

46. There are no direct sustainability implications arising from this report.

### **Equalities implications**

47. There are no direct equalities implications arising directly from this report.

48. Of course, the GDPR continues to provide extra protection to special categories of personal data (e.g. race, ethnic origin; religion; trade union membership; health; sexual orientation). Special category data is broadly similar to the concept of 'sensitive personal data' under the DPA 1998. The requirement to identify a specific condition for processing this type of data is also very similar.

49. One change is that the GDPR includes genetic data and some biometric data in the definition of sensitive data. Another change is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10 of GDPR.

50. The conditions for processing special category data under the GDPR in the UK are likely to be similar to the Schedule 3 conditions under the DPA 1998 Act for the processing of sensitive personal data.

### **List of Appendices to this report:**

General privacy notice

# General Privacy Notice

## Protecting your personal data and privacy

This privacy notice (sometimes called a fair processing notice) explains how the London Fire Brigade ("we" or "us") will use the personal data we hold about you. If we ask you for personal information we will hold a record of why we are asking and why the information is necessary to do our work.


We use the term 'privacy notice' to describe all the privacy information that we make available or provide to people when we collect information about them. Our privacy information is made up of:

- the privacy statement that we put on forms and letters
- our 'guide to privacy' leaflet
- This general privacy notice that explains;
  - why we use personal data,
  - information about us as a Data Controller
  - who the Data Protection Officer is and how to contact them,
  - your information rights and how to access the data we hold
  - consent
  - what to do if you have a concern about your data or privacy
- our Data protection and privacy policy (policy no. 351)

### Why we use personal information

When we collect and process information about you we do so according to UK data protection law. This means we will be fair and transparent about the data we collect and we will keep your information safe. Our main processing activities that use personal data are:

- **Emergency response** – providing an emergency response to fires and other emergencies
- **Fire safety and protection** – promoting fire safety and safe living, enforcing fire safety law, and to protect those who are vulnerable to harm
- **Youth activities** – working with young people
- **Public services** – providing people with services and information, and to respond to complaints or concerns
- **Business administration** – maintaining accounts and business records, and to manage contracts and services
- **Employment** – recruit, employ, manage, train, promote and retire our staff
- **Research** – carrying out research, surveys and to maintain a historical archive
- **Security** – using CCTV systems and body worn video devices (BWV) to keep our people and resources safe, and to prevent and detect crime
- **Media** – take photographs, video or use other audio-visual media
- **Communications** – maintaining our website, providing newsletters and information about our services
- **Legal** – complying with the law and to support local and national fraud initiatives.

We use this symbol  to help you to know when we are collecting personal information from you.

### **LFB as a Data Controller**

The London Fire Commissioner is the fire and rescue authority for London.. Our main address is: **London Fire Brigade, 169 Union Street, London SE1 0LL**. The main contact number is **020 8555 1200**.

We are a Data Controller for personal data. Our details have been registered with the Information Commissioners Office (ICO) and our register number is **Z7122455**. The ICO's register can be viewed online at <http://ico.org.uk>.

### **The Data Protection Officer**

Our **Data Protection Officer** (DPO) is the **Head of Information Management** (Mr D Wyatt) who has day-to-day responsibility for data protection and information governance issues. The DPO can be contacted via the address or phone number above, or by emailing **informationaccess@london-fire.gov.uk**.

### **Your information rights and how to access the data we hold**

When we use your personal data, you have rights about how that information is processed. Those rights include how you can access the information we hold, and how, in some situations, you can stop us from processing the information or have it corrected or deleted. For more information about your individual rights and the legislation that applies you can either contact us (as above), or contact the Information Commissioner (ICO). The ICO has a lot of information about data protection and your individual rights on their website which is <http://ico.org.uk>.

### **Consent**

You will often have a choice about what services you receive from us, but when we collect your personal information for that service – one of our main processing activities – we will often collect and retain your information because we have another duty or obligation to do so that does not require your consent.

When you give us your information on the basis that you give us your consent to use it (and not because of another processing obligation we have), then you can withdraw that consent at any time. If you wish to withdraw your consent for us to use your personal data then you should contact our Information Access Team who can be contacted via the address or phone number above, or by emailing **informationaccess@london-fire.gov.uk**. You should provide as much information as possible about the information you supplied, when it was given and the circumstances it was given in.

### **If you have a concern**

If you are unhappy with the way that your personal data has been used or any other aspect of how we have processed your information then please let us know. In the first instance you should contact our DPO who can investigate the matter for you and take any action that is necessary. You also have the right to raise your concern with the Information Commissioner. Details of how to make a complaint to the ICO are on their website at <http://ico.org.uk> or you can write to them at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.