LAW COMMISSION GENERAL DATA PROTECTION REGULATION POLICY AND GUIDE

Introduction

1.1 The Commission takes its responsibilities for the effective handling of personal data seriously. This policy sets out how we will meet our obligations under the General Data Protection Regulation (GDPR), which came into force in May 2018.

1.2 The Law Commission is an Arms' Length Body under the auspices of the Ministry of Justice. Our IT, HR policies and Financial reporting are all provided for using MoJ systems. Of particular importance, all Law Commission electronic records are stored either on personal MoJ-supplied computers or on the JustStore system. As the Law Commission is not a data controller in its own right, MoJ is the legal entity that must comply with the GDPR, and in relation to IT systems and Just-Store it is MoJ's responsibility to ensure they meet the requirements of the new data protection laws. However, many practical aspects of the new laws will still fall to the Law Commission.

1.3 The Law Commission is, however, a consultative organisation. It goes to the heart of how we work and our statutory functions are drafted with that in mind. It is therefore vital that we are able to process personal data so that we can contact our stakeholders and those with an interest in law reform. In so doing, we undertake to handle their personal information in accordance with the GDPR obligations and principles.

1.4 Law Commission projects are usually lengthy and often the same area of law will be considered on more than one occasion. The Commission will, therefore, retain personal data in line with our retention and deletion policies, via hard copy filing, electronic filing and a bespoke stakeholder management database unless we are asked to do otherwise.

Support

1.5 The Law Commission does not require its own Data Protection Officer (DPO); such support will be provided by the MoJ.

1.6 Any queries in relation to this policy should be referred to the Chief Executive in the first instance, who will request support from the DPO where required.

Personal data

1.7 The ICO guide to GDPR defines personal data as:

> *"The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.*
>
> *This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.*
>
> *The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data."*

Lawful basis

1.8 There are six lawful bases for processing information. Given the fundamental importance of consultation to the public functions that the Law Commission has a statutory basis for undertaking, the Commission has determined that the following two bases apply:

- **(c) Legal obligation:** processing is necessary for compliance with a legal obligation to which the controller is subject
- **(e) Public task:** 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.

1.9 This is based on our statutory obligation to keep the law under review and, specifically, the need to receive and consider law reform proposals, as stated in the Law Commissions Act 1965:

> *"Functions of the Commissions.*
>
> *(1) It shall be the duty of each of the Commissions to take and keep under review all the law with which they are respectively concerned with a view to its systematic development and reform, including in particular the codification of such law, the elimination of anomalies, the repeal of obsolete and unnecessary enactments, the reduction of the number of separate enactments and generally the simplification and modernisation of the law, and for that purpose—*
>
> *(a) to receive and consider any proposals for the reform of the law which may be made or referred to them;"*

1.10 The Law Commission would not be able to function unless it is able to consult widely on its proposals for law reform. The Commission has a wide range of professional and public consultees, many of whom will wish to be informed of law reform developments, either in specific areas of the law or more generally.

1.11 To be clear, however, the Law Commission will process personal data in accordance with the data protection principles in article 5 of the GDPR.

Consent

1.12 On the basis that the Commission is relying on the two bases above, it is not necessary for the Commission to obtain consent from those whose personal data we process.

Privacy notice

1.13 The Law Commission must continue to state to individuals why we retain their data; how we will process it; and, any rights which apply. The Law Commission's Privacy Notice is:

> *Under the General Data Protection Regulations (May 2018), the Law Commission must state the lawful bases for processing personal data. The*

Commission has a statutory function, stated in the 1965 Act, to receive and consider any proposals for the reform of the law which may be made or referred to us. This need to consult widely requires us to process personal data in order for us to meet our statutory functions as well as to perform a task, namely reform of the law, which is in the public interest. We therefore rely on the following lawful bases:

(c) Legal obligation: *processing is necessary for compliance with a legal obligation to which the controller is subject*

(e) Public task: *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.*

Law Commission projects are usually lengthy and often the same area of law will be considered on more than one occasion. The Commission will, therefore retain personal data in line with our retention and deletion policies via hard copy filing, electronic filing and a bespoke stakeholder management database unless we are asked to do otherwise. We will only use personal data for the purposes outlined above.

We may publish or disclose information you provide us in response to Law Commission papers, including personal information. For example, we may publish an extract of your response in Law Commission publications, or publish the response in its entirety. We may also share any responses received with Government. Additionally, we may be required to disclose the information, such as in accordance with the Freedom of Information Act 2000. If you want information that you provide to be treated as confidential please contact us first, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic disclaimer generated by your IT system will not be regarded as binding on the Law Commission. The Law Commission will process your personal data in accordance with the General Data Protection Regulations, which came into force in May 2018.

Any concerns about the contents of this Privacy Notice can be directed to: general.enquiries@lawcommission.gov.uk

1.14 The Privacy Notice should be displayed in all publications, consultation response forms, our website and via a link in all email signature blocks.

Redaction

1.15 GDPR does not materially affect the circumstances where it is necessary to redact personal data. This guidance is therefore based on the ICO document ‘How to disclose information safely’ It relates to the disclosure of information which has been derived from personal data and requires further processing to ensure that individuals cannot be identified from that information. There are several circumstances when the Commission should consider removing personal data:

- When responding to Subject access requests under the DPA;
- When proactively making information available under the Freedom of Information Act 2000 (FOIA);

- When responding to information requests under FOIA and disclosing third party personal data would breach one of the data protection principles; and,
- When redacting information that is outside the scope of an FOIA request is the most efficient way of releasing relevant information that should be disclosed.

1.16 Redaction – definition: The National Archives defines redaction as:

> *"the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. In the paper environment some organisations will know redaction as extracts when whole pages are removed, or deletions where only a section of text is affected."*

1.17 Care must be taken to ensure effective redaction; there are examples provided by the ICO whereby a marker pen used for redaction has not completely obscured text or, for digital information, text has been "hidden" by highlighting it in black, however, that can easily be reversed if information is sent out electronically rather than in hard copy. In terms of solutions, a black marker may not effectively redact information, but using a proper redaction pen and then photocopying or scanning the document will. Similarly, although redacting on Adobe may reversible, if you then print out the document and scan it, that is not reversible.

More details about how redactions can be dealt with in relation to consultation responses (and more generally) is available at **Annex A**.

1.18 Sharing within Government: In practical terms, if the personal data provided direct to the Commission is of a sensitive nature, for example, it reveals intimate details of an individual's private life, consideration should be given to redacting such personal information if it is not materially relevant or, where it is relevant, anonymising the information. The legal basis for the sharing of personal data within Government is dealt with below.

1.19 Third parties: Responding to a subject access request or FOIA request may involve providing information that relates both to the individual making the request and to another individual. Where the Commission cannot comply with the request without disclosing information relating to another individual who can be identified from that information, we are not obliged to comply with the request unless:

- (a) the other individual has consented to the disclosure of the information to the person making the request, or
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

1.20 It is unlikely the Commission will be able to obtain third party consent so our approach is likely to be to provide some information, having edited or redacted information that would identify them. See Appendix C for our guidance on redaction.

1.21 The general principle under GDPR, as with the Data Protection Act 1998, remains that the personal data of a third party should only be released (a) as part of a subject

access request; or, (b) as part of an FOI request if it has first been redacted to exclude all such third party personal data.

Stakeholder database

1.22 The Law Commission makes use of the Kahootz Stakeholder Management database for storing and processing personal data. The owners of that Database have confirmed the system meets all GDPR principles and obligations and have provided the assurances set out at **Annex B**. Any information entered into this system would be subject to both Subject Access Requests and, potentially, FoI requests.

Sharing agreement

1.23 Although independent, the Law Commission undertakes projects on behalf of Government Ministers. We maintain close working relationships with sponsoring Departments and, on occasion, will share consultation responses with that Department. This may include personal data. The ICO Code of Practice on Data Sharing suggests that the Law Commission has an implied power to share personal information:

> *"Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental", and then check that the organisation has the power to engage in that activity."*

1.24 The implied power arises from our statutory obligation to make recommendations to Government on law reform proposals, as defined in the 1965 Act. However, when asked to share data with a Government Department, you should consider whether the implied power covers the particular disclosure or data sharing in question

1.25 We make clear in our Privacy Notice that, if any consultee does not wish for their information to be shared we will do our utmost to abide by their wishes. If this is not possible, for example because to not provide the information would restrict our ability to undertake our statutory functions, advice should be sought from the MoJ Data Protection Officer.

1.26 On the basis that such sharing of data between the Commission and a Government Department is likely to be ad hoc, the Commission has decided that no general Data Sharing Agreement is required. In circumstances where it has been decided that, for a specific project, there will be routine sharing of personal data with the sponsoring Department, it may be good practice for the MoU to contain an annex detailing the specific arrangements which will apply. This should be based on the good practice set out in section 14 of the ICO Guide: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

1.27 We will not share personal information outside of Government unless specific consent is sought from affected individuals.

Data Protection breaches

1.28 The ICO GDPR guide defines a breach as:

> *"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.*
>
> *Example:*
> *Personal data breaches can include:*
>
> - *access by an unauthorised third party;*
> - *deliberate or accidental action (or inaction) by a controller or processor;*
> - *sending personal data to an incorrect recipient;*
> - *computing devices containing personal data being lost or stolen;*
> - *alteration of personal data without permission; and*
> - *loss of availability of personal data.*
>
> *A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals."*

1.29 Any personal data breach must be reported to the Chief Executive (or in their absence the Head of Corporate Services) immediately. It seems unlikely that any breach by the Commission would affect the rights and freedoms of individuals, in which case it is unlikely we would need to report the breach to the ICO. This determination will be made by the Chief Executive (or in their absence the Head of Corporate Services). This determination must be made within 72 hours and much sooner for any serious breach.

1.30 The Law Commission will record all breaches, regardless of whether or not they need to be reported to the ICO. This record should set out the facts relating to the breach, its effects and the remedial action taken.

1.31 As with any security incident, the Commission will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Subject access requests

1.32 Subject Access Requests continue in a similar vein to those undertaken under the Data Protection Act 1998 requirements. However, timescales and fees have changed. The ICO GDPR guide states:

"Under the GDPR, individuals will have the right to obtain:

- *confirmation that their data is being processed;*
- *access to their personal data; and*
- *other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).*

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

*You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.*

How long do I have to comply?

Information must be provided without delay and at the latest within one month of receipt. You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary."

Retention and deletion

1.33 The Law Commission has a Retention and Deletion Schedule, which has been updated to reflect the new Stakeholder Management System. It complies with GDPR requirements. It is available at **Annex C**.

Data Protection Impact Assessments (DPIA)

1.34 The GDPR guide states that DPIAs are:

> *"Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur."*

1.35 The circumstances in which a DPIA must be completed are when:

- using new technologies
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

1.36 In reality, there are unlikely to be any circumstances where the Commission must undertake a DPIA. However, in limited circumstances, it may be good practice, for example, if we are proposing a particularly largescale public consultation for a particular project or a smaller scale consultation on a subject that might result in individuals disclosing sensitive personal data or lead others to associate individuals with controversial or sensitive matters. This is likely to be very rare.

Compliance and corporate governance

1.37 This policy is intended comprehensively to set out how the Commission will meet its obligations under GDPR.

1.38 The Commission has less than 250 employees and therefore we only need to document data processing which is not occasional. This would apply to:

- Our consultations and stakeholder engagement in relation to individual projects and Programmes of law reform.
- Public correspondence
- Subject Access Requests
- FoI requests

1.39 The above categories are all routine aspects of our work. However, by way of example, we would not need to document processing of personal information in relation to an invitation to a Law Commission party because such an event would be classed as occasional.

1.40 The Commission will have in place an up to date:

- Information Asset Register
- Retention and Deletion Schedule
- Privacy Notice

Training

1.41 All Law Commission staff must undertake annually the Civil Service Learning online course: Responsible for Information.

Further sources of information:

- ICO GDPR guide: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- MoJ Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/
- Data Sharing: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

- Redactions: https://ico.org.uk/media/for-organisations/documents/how-to-disclose-information-safely-removing-personal-data-from-information-requests-and-datasets/2013958/how-to-disclose-information-safely.pdf

MAY 2018