HOUSE OF LORDS

# Data protection legislation: factsheet for Members of the House of Lords

## Overview

Under data protection legislation, you have special responsibilities when you and/or your staff handle data about living individuals ("personal data"). These responsibilities include keeping personal data secure. As with the Data Protection Act 1998, individual Members of the House of Lords are likely to be considered "controllers" of personal data under the UK General Data Protection Regulation. Individuals whose personal data are being processed ("data subjects") have certain rights, for example to ask to access the data.

## Contents

### Part 1 – Introduction to Data Protection legislation



### Part 2 – How does data protection legislation apply to Members of the Lords?



*This is version 4 of the factsheet (issued March 2021)*

# PART 1: INTRODUCTION TO DATA PROTECTION LEGISLATION

## What is the UK General Data Protection Regulation ("UK GDPR")?

The GDPR, as supplemented by the Data Protection Act 2018 ("DPA"), builds on and strengthens the framework of rights and duties designed to safeguard personal data introduced by the Data Protection Act 1998 (which has been repealed). It came into force on 25 May 2018. The GDPR has been retained in domestic law, with some amendments, following the end of the transition period for the UK leaving the EU. It is now known as the "UK GDPR".

## To what information does the UK GDPR apply?

The UK GDPR applies to "personal data". This means any information relating to an identifiable person who can be directly or indirectly identified, including by reference to an identifier (such as a national insurance number). Persons who process personal data must comply with the UK GDPR.

"Processing" is broadly defined as anything done to the data, including collecting, organising, storing, altering, sharing, using or destroying.

The UK GDPR does not apply to certain activities, including processing covered by the Law Enforcement Directive, processing for national security purposes and processing by individuals for purely personal or household activities.

## Controllers and processors – what is the difference?

The UK GDPR applies to "controllers" and "processors". A controller determines the purposes and means of processing personal data. A processor processes personal data on behalf of a controller, in accordance with the controller's instructions. Different requirements apply to controllers and to processors.

## Principles

The data protection principles set out in the UK GDPR are similar to those in the Data Protection Act 1998. The UK GDPR requires that personal data are:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

(f) processed in a manner that ensures appropriate security of the personal data.

**Lawful basis for processing**

There must be a lawful basis for processing personal data. The controller must ensure that one or more of the following grounds apply:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual.

(c) Legal obligation: the processing is necessary to comply with the law.

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest (which, under the Data Protection Act 2018, includes processing that is necessary in the exercise of a function of either House of Parliament or to carry out a task that supports or promotes democratic engagement).

(f) Legitimate interests: the processing is necessary for the legitimate interests of the controller or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The UK GDPR requires strict additional safeguards to be applied when processing 'special category personal data'. The categories of special personal data are:

> "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

Similar safeguards apply to personal data relating to criminal convictions and offences.

The ICO has produced more detailed guidance which is available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

The sample privacy notice relating to Members' parliamentary work suggests which legal bases may be relevant for individual Members engaging with members of the public.

**Individual rights**

The UK GDPR gives data subjects:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision making and profiling.

So, for example, where Members are acting as the controller, their responsibilities will include responding to requests from individuals for access to their personal data. The ICO has produced guidance on these rights which can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Responsibilities arising from a data subject's right to be informed are set out separately under "Privacy Notices" below.

## PART 2: HOW DOES DATA PROTECTION LEGISLATION APPLY TO MEMBERS OF THE LORDS?

When Members are acting as controllers, they must ensure that they process personal data in accordance with the UK GDPR. Members are likely to be controllers when (for example) they send or receive emails containing personal data:

- about employees or other persons who help them with their parliamentary duties;
- about Members of the public to help them take up a grievance with a government department.

If Members are unsure whether they are controllers in their own right they should seek advice from the Information Commissioner's Office (ICO). There is also information about this on the ICO's website: https://ico.org.uk/for-organisations/

### Contract

The UK GDPR requires Members who are controllers to enter into a contract with whoever does their data processing. Assuming Members use the parliamentary IT systems for processing personal data which relates to their parliamentary duties, they will need to have a contract with the Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons (acting jointly) who are responsible for Parliamentary Digital Services. The House Administrations have prepared a contract to reflect the requirements of the UK GDPR. The contract has been sent to each Member of the House; use of the parliamentary network on or after 25 May 2018 by a Member constitutes acceptance of the contract.

Notwithstanding the contract, Members remain personally liable for their compliance with the UK GDPR regarding the personal data they hold as controller. Failure to comply could have serious consequences: see the section below headed "breaches". Further information about this contract, which is in standard form for Members of both Houses, is given in a separate document.

### Taking up individual cases

Members may be approached by members of the public to take up their individual cases. Members may undertake activities in support of pressure groups and other organisations, including those relating to individual cases. In some instances, this may involve processing personal data or special categories of personal data.

If a Member wishes to disclose any special personal data, or data relating to criminal convictions or offences, to an organisation such as a government department, the Member must obtain the express consent of the individual concerned (the "data subject"). The Member will also need to keep a record of that consent.

## Privacy Notices

Where Members are acting as a controller, they will be responsible for providing data subjects with certain information, in the form of a privacy notice.

The House Administration has prepared two sample privacy notices which Members may wish to use.

Before you decide whether or not to use either notice, you must check carefully whether they meet your own circumstances and requirements. These notices relate to your own responsibilities as a controller of personal data under the UK GDPR, and you will be responsible for the content of each notice if you decide to use them.

*Notice for Members' staff*

If you employ someone to support your parliamentary work you will be the controller of personal data about that person, even if you are not legally their employer.

A privacy notice which you can provide to staff in these cases is available as a Word document on the intranet, or from the Information Compliance team. Before use the Member must check it and add their own name and contact details.

*Notice for communications with the public*

When you communicate with a member of the public who asks you to raise a particular issue, or to help them with a problem because you are a Member of the Lords, you are the controller of the personal data provided by the person.

The House Administration has put on the Parliamentary website a standard privacy notice for these situations. If you are content with it, you can simply provide people with a link to this standard notice.

To do this, Members may wish to add some standard text to their e-mail signatures from their Parliamentary accounts. This means that you will automatically provide data protection information every time you send an e-mail. Here is some suggested standard text – a shorter version and a longer version. Either version should be acceptable.

| |
|---|
| *Possible text to add to your e-mail signature: short version*<br><br>If you send me personal data in connection with my parliamentary work, click here for data protection info. |
| Note: if you cannot add the internet link in the word "here" (it is hard to add these kind of links on iPhones or iPads), put "click link for data protection info", and then give the full link.<br>https://www.parliament.uk/site-information/data-protection/house-of-lords-members-data-protection-information/ |

*Possible text to add to your e-mail signature: longer version*

Data protection: if you send me personal data in connection with my parliamentary duties, I have a duty to protect that data. Under data protection legislation, you have rights in relation to your personal data. If you would like more information, please click here

If you would like help to add this standard text to your Parliamentary e-mail signature, staff of the PDS drop-in centre on the First Floor West Front corridor will be pleased to help, as will the helpdesk staff on x2001.

If you want the standard text to appear on more than one device, you will need to set it up on each device separately. Again, PDS can advise.

If you are not satisfied with the wording of the privacy notice on the Parliamentary website, the text is also available as a Word document on the intranet, or from the Information Compliance team. You can adapt it and use it as you wish. (You could for example adapt one of the e-mail signatures above, to indicate that privacy information is available from you on request.)

## Data security

See the "cyber security" pages on the intranet for guidance which will help to keep personal data secure.

For example, Members should set a secure password, follow the "User Responsibilities" requirements, and delete e-mails and other electronic files containing personal data when they are no longer needed.

The Parliamentary Digital Service can provide cyber security advice for Members, either at the drop-in centre on the First Floor West Front Corridor, or on tel. x2001.

**Retention**

Members should consider for how long personal data contained in e-mails, files on their computers or letters should be retained, and when such data should be deleted.

The data protection legislation does not specify time periods after which personal data must be deleted, so firm advice cannot be given about this. Instead the legislation sets out principles for holding personal data. These principles apply whether the personal data are held in emails, or in electronic or hard-copy files.

These principles include that personal data should be:

- collected for specific purposes and held only for those purposes
- relevant and limited to what is necessary in relation to the purposes for which the data are held
- accurate and where necessary kept up to date.

In general, personal data should be held only for as long as it is necessary to hold them. Personal data should not be held indefinitely just in case they might be useful in future.

You should use these principles to develop your own simple routines for retaining then deleting different types of material. Here are some examples:

- If you receive an unsolicited circular on which you will take no action you might delete that email immediately. (NB when you delete an e-mail from your inbox it goes to the "deleted items" folder. Periodically delete everything in your "deleted items" folder.)

- If you hold personal data for the purpose of organising an event in Parliament you might delete those data soon after the event has taken place – unless there are good reasons for retaining the data for longer in the case of particular individuals, perhaps because you wanted to engage further with them about the subject of the event.

- Personal data about an individual's case you may be pursuing might be held until you think that the case has finally concluded. If you thought it possible that the person would contact you again, and that you would need the data if they did so, then it would be reasonable to keep the data for a period of time – this could extend to years, if you think it reasonable, but it should not be indefinite.

- Personal data on those you employ might be held for the duration of their employment and some time afterwards (for example, so that you can provide a reference to another employer or, if necessary, give tax information to HMRC). Such personal data may be held for many years if the data relate to an employee's pension.

## Charges payable to the Information Commissioner

The Data Protection (Charges and Information) Regulations 2018, which require most controllers to pay an annual charge to the Information Commissioner, have been amended.

Following a public consultation last year, as of 1 April 2019 Members will no longer be required to pay the charge to the Information Commissioner in respect of processing of personal data in relation to their parliamentary duties. This exemption also covers Members' staff acting solely in this capacity.

It should be noted that Members still have to comply with the UK GDPR, as supplemented by the DPA 2018, in relation to their parliamentary duties.

Members who process personal data in relation to their outside interests may need to pay the charge. The Information Commissioner's Office has a **self-assessment tool** to help individuals decide whether or not they need to pay the fee:

Advice is also available from the ICO's helpline: 0303 123 1113.

## Breaches

Where Members are acting as the controller, they will be responsible for reporting notifiable data breaches to the ICO. A notifiable breach is one which is likely to result in a risk to the rights and freedoms of the individuals whose data have been compromised. A notifiable breach must be reported to the ICO without undue delay, and not later than 72 hours after the controller becomes aware of it. Where the effect of a data loss is particularly serious, the controller will also be required to notify the data subject.

The UK GDPR and DPA confer wide powers on the ICO to enforce the new data protection legislation. These include the power to impose substantial fines on a controller or processor who has breached a requirement of the UK GDPR. In addition, individuals whose data is lost as a result of that breach may be able to sue the controller and/or the processor for compensation as a result of any damage suffered. In some cases, compensation may also be payable for distress caused by a breach.

If personal data controlled by a Member were lost from the parliamentary IT systems, a court or tribunal may have to determine whether the loss was due to the fault of the Member as controller or the Corporate Officers as processor, and who should pay any fines, damages or costs.

More information is available at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

## Parliamentary privilege

The Data Protection Act 2018 contains provisions designed to protect Parliamentary privilege. These ensure in particular that it will be lawful for a Member to disclose personal

data about a third party during a speech to the House or in other Parliamentary proceedings, even without that person's consent.

The Act also restricts some of the rights conferred by the UK GDPR on data subjects where Parliamentary privilege applies. For example, an individual would not have the right to seek access to notes prepared by a Member for a speech given in the House which contained the individual's personal data.

The Information Commissioner has no power to take action against a Member where to do so would involve the infringement of Parliamentary privilege – for example, by seeking to require a Member to hand over material that the Member had prepared for the purposes of a debate in the House.

Parliamentary privilege protects proceedings in Parliament: it does not normally apply to communications between a member of the public and a Member of the House, nor between an employee and a Member.

**Further advice**

The UK regulatory body is the Information Commissioner's Office. Their website contains a great deal of advice and guidance:
www.ico.org.uk

The Parliamentary intranet has resources to help Lords Members to meet obligations under data protection legislation:
https://intranet.parliament.uk/information-management/data-protection-security/data-protection/gdpr-for-lords-members/

The Lords Information Compliance team may be able to advise about the particular context of the House of Lords:

e-mail holinfocompliance@parliament.uk
tel 020-7219 0100 / 8481

**Checklist**

This checklist provides a starting point for Lords Members. For further info on each item, see the relevant section of this Guide.

1. **Understand the purpose of the data protection legislation**: read through this factsheet (and Information Commissioner's Office guidance)

2. **Contract**: if you are content with the contract in the information pack issued to all Members on 9 May, and available on the intranet, you do not need to do anything further with this: it automatically covers your obligation to have a contract in place with us (the House Administration) as your data processor

3. **Staff?** If you employ someone in respect of your parliamentary work, check the sample "employees" privacy notice, edit it if necessary, and provide it to your employee

4. **Communicating with the public?** To provide privacy information when communicating with members of the public about your parliamentary work, you can add an automatic e-mail signature, signposting people to the "parliamentary work" privacy notice

5. **Data security**: use the Parliamentary Network, which has good security measures in place. Follow advice e.g. on setting secure passwords

6. **Retention**: Develop a simple process for deciding how long you will keep different types of personal data

7. **Charge?** Decide whether you need to pay a charge to the ICO in respect of your non-parliamentary interests.

Updated March 2021