



BRIEFING PAPER

Number 1936, 31 October 2018

Data protection: constituency casework

By John Woodhouse

Contents:

1. The General Data Protection Regulation
2. The Data Protection Act 2018 and MP's casework
3. Further information



Contents

Summary	3
1. The General Data Protection Regulation	4
What is personal data?	4
What is data processing?	4
When can personal data be lawfully processed?	5
When can special category personal data be lawfully processed?	5
How should personal data be processed?	6
What rights do data subjects have?	7
2. The Data Protection Act 2018 and MP's casework	8
Members and special categories of personal data	8
3. Further information	10

Summary

The [General Data Protection Regulation](#) (GDPR) and the [Data Protection Act 2018](#) now form the UK's data protection regime.

Under the GDPR, Members of Parliament are data controllers. Any processing of personal data by Members must comply with the GDPR and the 2018 Act. This means that personal data can only be processed if there is a lawful basis for doing so. The lawful bases are:

- **Consent:** an individual has given clear consent for the processing of their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract between an individual and an organisation.
- **Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect an individual's personal data which overrides those legitimate interests.

Members' casework and special category data

Special category personal data includes data revealing a person's racial origin, ethnic origin, health details, sexual orientation, and political and philosophical beliefs. Schedule 1 of the 2018 Act sets out a number of areas in which the processing of special category personal data is permitted without an individual's explicit consent.

For Members of Parliament (and other elected representatives), paragraphs 23 and 24 of Schedule 1 have two main functions that apply when a constituent has contacted them.

[Paragraph 23](#) sets out when a Member of Parliament (or someone acting with their authority) can process certain "special category" data about an individual, in the course of the Member's "functions as a representative" (e.g. constituency casework), without having to establish explicit consent.

[Paragraph 24](#) allows, but does not require, others (e.g. agencies or organisations) who are contacted by Members to disclose special category personal data to them where this is necessary to help with their functions, without having to obtain the explicit consent of the individual concerned.

Sources of advice

The [Information Commissioner's Office](#) (ICO) oversees data protection law. Guidance for elected representatives is available from the ICO [website](#). The ICO can discuss individual cases - its [advice line](#) is 0303 123 1113.

The House has an [Information Rights and Information Security](#) (IRIS) Service. IRIS has published [information](#) [intranet only] for Members. IRIS can provide advice to Members and their staff on the application of data protection law.

1. The General Data Protection Regulation

The [General Data Protection Regulation](#) (GDPR) has applied directly in Member States from 25 May 2018. The Regulation sets out the responsibilities of:

- [data controllers](#) - the persons or bodies that determine the purposes and means of processing of personal data; and
- [data processors](#) - those who process personal data on behalf of a controller.

It also details the rights of “data subjects” - the individuals whose personal data is being processed.

The [Data Protection Act 2018](#) sets out, among other things, how the Government has chosen to apply derogations allowed under the GDPR.

What is personal data?

Personal data is any information relating to an identified or identifiable living individual.¹ Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data.

Examples of personal data include:

- a name and surname;
- a home address;
- an email address such as [name.surname@company.com](#);
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.²

What is data processing?

Article 4(2) of the GDPR defines processing as:

(...) any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by

¹ Article 4(1) of the GDPR

² European Commission website, [What is personal data?](#) [accessed 29 October 2018]

automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

When can personal data be lawfully processed?

Personal data can only be processed if there is a lawful basis for doing so. Under Article 6 of the GDPR, the lawful bases are:

- **Consent** – an individual has given consent to the processing of his or her personal data for one or more specific purposes
- **Contract** - 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
- **Legal obligation** – processing is necessary for compliance with a legal obligation to which a data controller is subject
- **Vital interests** - processing is necessary to protect someone's life
- **Public task** – processing is necessary for the performance of a task carried out in the public interest or for official functions and the task or function has a clear basis in law.
- **Legitimate interests** - the processing is necessary for a data controller's legitimate interests 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.

In March 2018, the ICO published guidance on [legitimate interests](#) and on [consent](#).

When can special category personal data be lawfully processed?

Article 9(1) of the GDPR prohibits the processing of special categories of personal data. This is data that reveals an individual's:

- Racial origin
- Ethnic origin
- Political opinions
- Religious beliefs
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data

6 Data protection: constituency casework

- Data concerning a natural person's sex life
- Sexual orientation

The above types of personal data were known as “sensitive personal data” under the *Data Protection Act 1998* (now repealed).

Article 9(2) allows the processing of special category data if certain conditions are met. One of these is that the data subject has given “explicit consent” to the processing.³

How should personal data be processed?

Article 5 of the GDPR lists the following principles for the processing of personal data:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**‘purpose limitation’**);

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**‘accuracy’**);

(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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**‘storage limitation’**);

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

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**‘accountability’**).

³ Article 9(2)(a)

What rights do data subjects have?

Strengthened consent is one of the major changes that the GDPR makes for data subjects. Article 4 (11) defines consent as follows:

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The definition's references to "unambiguous" and "clear affirmative action" are new. A data controller must be able to demonstrate that a data subject has consented to the processing of their personal data. It must be possible to withdraw consent at any time.⁴

The GDPR enhances the rights of data subjects in a number of other ways including:

- Right of access - the right to obtain confirmation from a data controller as to whether or not their personal data is being processed, where and for what purpose⁵
- Right to erasure – the right to obtain from a data controller the erasure of personal data if certain conditions are met e.g. the data no longer being relevant to the original purposes for processing, the data subject withdrawing consent, the data being unlawfully processed⁶
- Mandatory breach notification - where a data breach is likely to result in a "high risk to the rights and freedoms" of data subjects⁷
- The right not to be subject to a decision based solely on automated processing⁸

The right of access means that a constituent can ask to see the personal information that an MP's office holds on them.

The ICO [website](#) and the European Commission [website](#) include further detail on individuals' rights.

An ICO [guide](#) (August 2018) explains what data controllers need to do to comply with the GDPR.

⁴ Article 7

⁵ Article 15

⁶ Article 17

⁷ Article 34

⁸ Article 22

2. The Data Protection Act 2018 and MP's casework

Members of Parliament are data controllers under the GDPR.⁹ Any processing of personal data by Members must comply with the GDPR and the 2018 Act. One of the Act's purposes is to set out how the UK has applied the derogations available under the GDPR.

As noted earlier, personal data can be processed where there is a lawful basis for doing so i.e. consent, legal obligation, vital interests, public task, legitimate interests.

Members and special categories of personal data

Schedule 1 of the 2018 Act sets out a number of areas in which the processing of the special categories of personal data is permitted.

For Members of Parliament (and other elected representatives), paragraphs 23 and 24 of Schedule 1 have two main functions that apply when a constituent has contacted an MP.

Paragraph 23 of Schedule 1

Under [paragraph 23](#), an MP (or someone acting with their authority) can process special category personal data about a constituent, in the course of the Member's "functions as a representative" (e.g. constituency casework), without having to establish "explicit consent". However, this processing will only be lawful in two sets of particular circumstances.

The first is where the individual whose information is being processed has made the request himself or herself, and the data processing is necessary to help with action reasonably taken in response to that request.

The second set of circumstances applies if the request is made by someone other than the data subject. Here, the data can be processed without explicit consent, but only if this is necessary for one of the following reasons:

- a. in the circumstances, consent to the processing cannot be given by the data subject;
- b. in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;
- c. obtaining the consent of the data subject would prejudice the action taken by the elected representative;
- d. the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

⁹ ICO website, [Elected representatives and political parties](#) [accessed 29 October 2018]

Paragraph 24 of Schedule 1

[Paragraph 24](#) sets out the circumstances in which information can be (but does not have to be) disclosed to MPs. It mirrors the circumstances in which the MP or their staff can process the data.

If it is the data subject who has made the request to the MP, then the data holder could disclose information in response to the MP's communication so long as the personal data is relevant to the subject matter of that communication, and the disclosure is necessary to respond to that communication.

In the case of the request coming from someone else, the disclosure could only be made without the data subject's consent in one of the following circumstances:

- a. in the circumstances, consent to the processing cannot be given by the data subject;
- b. in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;
- c. obtaining the consent of the data subject would prejudice the action taken by the elected representative;
- d. the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

3. Further information

The [Information Commissioner's Office](#) (ICO) oversees data protection law. Guidance for elected representatives is available from the ICO [website](#). A range of other material on the GDPR, the 2018 Act, and the rights of data subjects is available from the ICO site.

The ICO can discuss individual cases - its [advice line](#) is 0303 123 1113.

The House has an [Information Rights and Information Security](#) (IRIS) Service. IRIS has published [information](#) [intranet only] for Members. IRIS can provide advice to Members and their staff on the application of data protection law

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer

This information is provided to Members of Parliament in support of their parliamentary duties. It is a general briefing only and should not be relied on as a substitute for specific advice. The House of Commons or the author(s) shall not be liable for any errors or omissions, or for any loss or damage of any kind arising from its use, and may remove, vary or amend any information at any time without prior notice.

The House of Commons accepts no responsibility for any references or links to, or the content of, information maintained by third parties. This information is provided subject to the [conditions of the Open Parliament Licence](#).