HOUSE OF LORDS Library Briefing

Personal Data, Social Media and Election Campaigns
Debate on 14 June 2018

Summary

This Briefing has been prepared in advance of the debate due to take place in the House of Lords on the motion moved by Lord Knight of Weymouth (Labour) that "this House takes note of the use of personal data harvested from social media sites in recent election campaigns and Her Majesty's Government's response to this".

Concerns have been expressed that personal data gathered from social media may have been used to target political messaging in ways which are not sufficiently transparent. Allegations have also been made concerning the use in recent election campaigns of personal data which may have been improperly taken from social media sites.

These allegations are being investigated by various bodies. The Information Commissioner has opened an investigation into "the use of data analytics for political purposes". The House of Commons Digital, Culture, Media and Sport Committee is currently conducting an inquiry into "fake news", as part of which it has taken evidence regarding the use of personal data taken from social media sites in election campaigns. The Electoral Commission is also undertaking inquiries into whether payments for services of data companies breached campaign spending limits, and into the use of digital campaigning in elections. These inquiries are on-going.

There have been several recent developments in data protection legislation. The European Union legislation the General Data Protection Regulation (GDPR) is directly applicable in the UK, and came into effect in May 2018. Parliament has passed the Data Protection Act 2018, which makes use of several available derogations in the GDPR. These pieces of legislation provide enhanced individual rights over personal data, and protections concerning the processing of sensitive personal data. The European Union (Withdrawal) Bill will preserve the GDPR in domestic legislation, and the Government has stated its intention to maintain high data protection standards after the UK's exit from the EU.

Table of Contents

Emily Haves
7 June 2018

Table of Contents

---

1. Inquiries into Personal Data and Political Campaigning

1.1 Allegations

In recent years concerns have been expressed that data gathered from social media, and other sources, may have been used to target political messaging in ways which are not sufficiently transparent. For example, in February 2017 the *Guardian* reported that data analytics firms had worked with political campaigns to target political advertising based on personal data held by Facebook, the social media company.[1]

In March 2018, allegations were also made that certain companies, including Cambridge Analytica (UK) Limited (now in administration) and the Canadian-based company AggregateIQ, used personal data gathered from social media and subsequently shared without the required permissions in order to place targeted political messages.[2] These claims are disputed by Cambridge Analytica and AggregateIQ.[3] In a statement made in April 2018, Facebook estimated that the personal information of 87 million of its users "may have been improperly shared with Cambridge Analytica".[4] Of these, Facebook estimated that 81.6 percent (70.6 million people) were based in the USA, and 1.2 percent (1.1 million people) were based in the UK. These allegations particularly relate to targeted political advertising during the 2016 US presidential election.

1.2 Information Commissioner's Investigation

In May 2017, in response to concerns about how personal data is used in political campaigns, the Information Commissioner opened a formal investigation into "the use of data analytics for political purposes".[5] In an interview with the BBC, the Information Commissioner, Elizabeth Denham, said:

> What we're looking at here, and what the allegations have been about, is mashing up, scraping, using large amounts of personal data, online data, to micro target or personalise or segment the delivery of the

---

[1] Carole Cadwalladr, 'Robert Mercer: The Big Data Billionaire Waging War on Mainstream Media', *Guardian*, 26 February 2017.
[2] Zoe Kleinman, 'Cambridge Analytica: The Story So Far', BBC News, 21 March 2018; and Jane Wakefield, 'Canada Data Firm AIQ May Face Legal Action in UK', BBC News, 26 April 2018.
[3] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *Guardian*, 17 March 2018; and Carole Cadwalladr, 'AggregateIQ: The Obscure Canadian Tech Firm and the Brexit Data Riddle', *Guardian*, 31 March 2018.
[4] Mike Schroepfer, 'An Update on Our Plans to Restrict Data Access on Facebook', Facebook, 4 April 2018.
[5] Elizabeth Denham, 'The Information Commissioner Opens a Formal Investigation into the Use of Data Analytics for Political Purposes', Information Commissioner's Office Blog, 17 May 2017.

> messages without individuals' knowledge. I think the allegation is that fair practices and fair democracy is under threat if large data companies are processing data in ways that are invisible to the public.[6]

Writing about the purpose of this investigation, the Information Commissioner said:

> This is a complex and rapidly evolving area of activity and the level of awareness among the public about how data analytics works, and how their personal data is collected, shared and used through such tools, is low. What is clear is that these tools have a significant potential impact on individuals' privacy. It is important that there is greater and genuine transparency about the use of such techniques to ensure that people have control over their own data and the law is upheld.[7]

In an update on the investigation published in December 2017, the Information Commissioner highlighted the wide-ranging and multifaceted nature of the investigation, stating:

> It's a complex and far-reaching investigation, involving over 30 organisations including political parties and campaigns, data companies and social media platforms. Among those organisations is AggregateIQ, a Canadian-based company, used by a number of the campaigns.[8]

Giving evidence to the House of Commons Digital, Culture, Media and Sport Committee in March 2018, the Information Commissioner explained that there were two elements to the investigation:

> What we are trying to do in this investigation really falls along two tracks. On the first track, our intention is to be able to pull back the curtain and explain and expose for the public, parliamentarians and civil society what happens with their personal information in the context of political advertising and political messaging. The second track of our investigation is, if we find contraventions of the Data Protection Act, we will be taking enforcement action. That enforcement action could take some time.[9]

---

[6] Gabriel Gatehouse, 'Did Cambridge Analytica Play a Role in the EU Referendum?', BBC News, 27 June 2017.
[7] Elizabeth Denham, 'The Information Commissioner Opens a Formal Investigation into the Use of Data Analytics for Political Purposes', Information Commissioner's Office Blog, 17 May 2017.
[8] Elizabeth Denham, 'Update on ICO Investigation into Data Analytics for Political Purposes', 13 December 2017.
[9] House of Commons Digital, Culture, Media and Sport Committee, *Oral evidence: Fake News*, 6 March 2018, HC 363 of session 2017–19, Q895.

In her most recent update, made on 5 April 2018, the Information Commissioner said:

> As part of my investigation into the use of personal data and analytics by political campaigns, parties, social media companies and other commercial actors, the ICO is investigating 30 organisations, including Facebook.
>
> The ICO is looking at how data was collected from a third party app on Facebook and shared with Cambridge Analytica. We are also conducting a broader investigation into how social media platforms were used in political campaigning.
>
> Facebook has been cooperating with us and, while I am pleased with the changes they are making, it is too early to say whether they are sufficient under the law.
>
> This is an important time for privacy rights. Transparency and accountability must be considered, otherwise it will be impossible to rebuild trust in the way that personal information is obtained, used and shared online.
>
> This is why, besides my investigation, which could result in enforcement action, I will also be making clear public policy recommendations to help us understand how our personal data is used online and what we can do to control how it's used.[10]

Ms Denham said she expected that her report into the use of personal data in political campaigns to be published in the spring of 2018.[11]

1.3 House of Commons Digital, Culture, Media and Sport Committee Inquiry

On 30 January 2017, the then House of Commons Culture, Media and Sport Committee launched an inquiry into "fake news", which it described as "the growing phenomenon of widespread dissemination, through social media and the internet, and acceptance as fact of stories of uncertain provenance or accuracy".[12] This inquiry was closed when Parliament was dissolved ahead of the 2017 general election, however the House of Commons Digital, Culture, Media and Sport Committee of the 2017 parliament is continuing this work

[10] Information Commissioner's Office, 'ICO Statement: Investigation into Data Analytics for Political Purposes', 2 May 2018.
[11] House of Commons Digital, Culture, Media and Sport Committee, *Oral evidence: Fake News*, 6 March 2018, HC 363 of session 2017–19, Q895.
[12] House of Commons Digital, Culture, Media and Sport Committee, "'Fake News" Inquiry Launched', accessed 29 May 2018.

with its own inquiry into the same topic.[13]

As part of this inquiry, the Committee has taken evidence from Christopher Wylie, who was formerly associated with Cambridge Analytica, regarding the use of personal data taken from social media sites in election campaigns.[14] This inquiry is on-going.

1.4 Electoral Commission Inquiry

Allegations have also been made regarding whether campaign spending limits were breached during the 2016 referendum by various groups paying for the services of AggregateIQ, the Canadian digital advertising, web and software development company.[15] These claims are disputed, and are being investigated by the Electoral Commission.[16]

The Electoral Commission is also undertaking inquiries into the use of digital campaigning in elections. Writing on the Electoral Commission blog, Bob Posner, Electoral Commission Director of Political Finance and Regulation and Legal Counsel, wrote that these inquiries cover a broad range of topics:

> Utilising our experience of regulating the Scottish Independence Referendum, the EU Referendum and the recent general elections, we are considering the use of digital campaigning alongside our electoral system. We are taking a wide definition of digital campaigning for these enquiries, including the use of data held by parties, campaigners and social media companies to target campaign messages, how political ads are used on social media, and the use of automated bots.[17]

1.5 Government Response

On 19 March 2018, Damian Collins (Conservative MP for Folkestone and Hythe) asked an urgent question regarding the use of personal data by Cambridge Analytica and the Information Commissioner's investigation:

> To ask the Secretary of State for Digital, Culture, Media and Sport to make a statement about the alleged breach of Facebook user data by Cambridge Analytica and the powers of the Information Commissioner

---

[13] House of Commons Culture, Media and Sport Committee, 'What Is "Fake News"?', 15 September 2017.
[14] House of Commons Digital, Culture, Media and Sport Committee, 'Fake News Inquiry—Publications', accessed 29 May 2018.
[15] Brian Wheeler, 'Brexit: Electoral Commission Reopens Probe into Vote Leave', BBC News, 20 November 2017.
[16] Electoral Commission, 'Electoral Commission Statement Regarding Vote Leave Limited, Mr Darren Grimes and Veterans for Britain Limited', 20 November 2017.
[17] Bob Posner, 'Responding to the Rise of Digital Campaigning', Electoral Commission Blog, 31 October 2017.

> to act in such cases.[18]

In response, the Secretary of State for Digital, Culture, Media and Sport, Matt Hancock, emphasised the severity of the allegations, stating: "the revelation this weekend of a serious alleged privacy breach involving Facebook data is clearly very worrying".[19] He stated that such matters were the purview of the Information Commissioner, and emphasised that stronger enforcement powers for the Information Commissioner formed part of the Data Protection Bill then progressing through Parliament:

> In our increasingly digital world, it is essential that people can have confidence that their personal data will be protected. The Information Commissioner, as the data regulator, is already investigating as part of a broader investigation into the use of personal data during political campaigns. The investigation is considering how political parties and campaigns, data analytics companies and social media platforms in the UK have used people's personal information to micro-target voters. As part of the investigation, the Commissioner is looking at whether Facebook data was acquired and used illegally.
>
> […]
>
> Data, properly used, has massive value, and social media are a good thing, so we must not leap to the wrong conclusions and shut down all access. We need rules to ensure transparency, clarity and fairness, and that is what the Data Protection Bill will provide. After all, strong data protection laws give citizens confidence, and that is good for everyone.

On 27 March 2018, Lord Taylor of Warwick (Non-affiliated) tabled a parliamentary question concerning the use of personal data by Cambridge Analytica and the Government's response:

> To ask Her Majesty's Government what assessment they have made of the use of data by Cambridge Analytica; and how they will ensure protection of personal data.[20]

Responding for the Government, Lord Ashton of Hyde, Parliamentary Under Secretary of State for the Department for Digital, Culture, Media and Sport, said:

> Cambridge Analytica's use of data is the subject of an investigation by the independent Information Commissioner. Questions about that investigation should be directed to the Information Commissioner's

---

[18] HC *Hansard*, 19 March 2018, col 49.
[19] ibid.
[20] House of Lords, 'Written Question: Cambridge Analytica: Data Protection', 27 March 2018, HL6722.

> Office.
>
> The Government's Data Protection Bill will strengthen data protection law and give the Information Commissioner tougher powers to ensure organisations comply. It will enhance control, transparency and security of data for people and businesses across the UK, and gives the Information Commissioner the power to levy significant fines against organisations that break data protection law or block her investigations.

2. Data Protection: Government Policy

2.1 Conservative Party Manifesto 2017

The Conservative Party manifesto published ahead of the 2017 general election stated that the Party would, if returned to government, ensure that the UK was the "global leader in the regulation of the use of personal data and the internet".[21] It stated that a Conservative government would:

> […] give people new rights to ensure they are in control of their own data, including the ability to require major social media platforms to delete information held about them at the age of 18, the ability to access and export personal data, and an expectation that personal data held should be stored in a secure way.[22]

The manifesto added that a Conservative administration would "bring forward a new data protection law, fit for our new data age", to ensure the "very best standards for the safe, flexible and dynamic use of data and enshrining our global leadership in the ethical and proportionate regulation of data".[23]

2.2 Queen's Speech 2017

Following the undertakings made in the Conservative manifesto, the Government announced in the June 2017 Queen's Speech that it would bring forward a "new law [to] ensure that the United Kingdom retains its world-class regime protecting personal data".[24] Government briefing notes published alongside the Queen's Speech stated that the Bill would:

- ensure that our data protection framework is suitable for our new digital age, and cement the UK's position at the forefront of technological innovation, international data sharing and protection of personal data;

---

[21] Conservative Party, *Conservative Party Manifesto 2017*, May 2017, p 38.
[22] ibid, p 79.
[23] ibid, p 80.
[24] HL *Hansard*, 21 June 2017, col 6.

- strengthen rights and empower individuals to have more control over their personal data including a right to be forgotten when individuals no longer want their data to be processed, provided that there are no legitimate grounds for retaining it;
- establish a new data protection regime for non-law enforcement data processing, replacing the Data Protection Act 1998; and
- modernise and update the regime for data processing by law enforcement agencies.[25]

2.3 Recent Developments

The Data Protection Bill [HL] was introduced in the House of Lords on 13 September 2017 and received royal assent on 23 May 2018, becoming the Data Protection Act 2018. Further information regarding the Act is given in section 3 of this Briefing.

On 11 April 2018, the *Guardian* reported that the Secretary of State for Digital, Culture, Media and Sport, Matt Hancock, had met with representatives of the social media firm Facebook to discuss its custodianship of personal data.[26] The newspaper reported that Mr Hancock had suggested that social media firms could be further regulated in this regard in the future. He said:

> Social media companies are not above the law and will not be allowed to shirk their responsibilities to our citizens. We will do what is needed to ensure that people's data is protected and don't rule anything out—that includes further regulation in the future.[27]

The Government has stated that it intends to continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows after the UK leaves the European Union.[28] In May 2018, the Government published a presentation which emphasised its commitment to high standards of data protection and stated its ambition to achieve an agreement with the EU which builds on the existing adequacy model.[29]

---

[25] Prime Minister's Office and Cabinet Office, *Queen's Speech 2017: Background Briefing Notes*, 21 June 2017, p 16.
[26] Heather Stewart, 'Act on Data Privacy or We'll Regulate, UK Minister Tells Facebook', *Guardian*, 11 April 2018.
[27] ibid.
[28] HM Government, *The Exchange and Protection of Personal Data—A Future Partnership Paper*, 24 August 2017, p 2.
[29] HM Government, *Framework for the UK-EU Partnership: Data Protection*, 23 May 2018, p 16.

3. General Data Protection Regulation and Data Protection Act 2018

3.1 Background to the General Data Protection Regulation

In January 2012, the European Commission proposed reform of data protection rules across the EU in order to strengthen online privacy rights and boost Europe's digital economy.[30] In April 2016, the General Data Protection Regulation (GDPR) was adopted by the European Council and European Parliament, and the deadline for its full application was 25 May 2018.[31] The European Commission has stated that the GDPR is "an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the digital single market".[32]

3.2 GDPR and Data Protection Act 2018: Purpose and Main Provisions Relating to Commercial Use of Personal Data

The GDPR regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.[33] Personal data is defined as any information relating to an identified or identifiable natural person.[34] Processing of data has a wide definition in the legislation, which states:

> 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by 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.[35]

The GDPR sets out the conditions under which data can be lawfully processed, which are that:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

---

[30] European Commission, 'The History of the General Data Protection Regulation', accessed 30 May 2018.
[31] ibid.
[32] European Commission, 'Protection of Personal Data', accessed 30 May 2018.
[33] European Commission, 'What Does the General Data Protection Regulation (GDPR) Govern?', accessed 30 May 2018.
[34] Regulation (EU) 2016/679, Article 4(1).
[35] Regulation (EU) 2016/679, Article 4(2).

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

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

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

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[36]

The GDPR also provides enhanced rights for individuals concerning their data:

- Individuals have the right to be informed about the collection and use of their data. The data controller must provide individuals with information including the purpose of processing the data, how long it will be retained for, and who it will be shared with.[37]
- Individuals have the right to access their personal data.[38]
- Individuals have the right to rectify information held about them if it is inaccurate, or to have it completed if it is incomplete.[39]
- Individuals have the right to have their personal data erased under certain circumstances.[40]
- Individuals have the right to restrict the processing of their personal data under certain circumstances.[41]
- Individuals have the right to data portability. This gives data subjects the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format.[42]
- Individuals have the right to object to the processing of their personal data, which requires the data controller to stop it being processed. This is an absolute right in the case of direct marketing, otherwise it is subject to limitations.[43]
- Individuals also have rights related to automated decision making and profiling, which is only allowed under specific

[36] Regulation (EU) 2016/679, Article 6(1).
[37] Information Commissioner's Office, 'Right to Be Informed', accessed 5 June 2018.
[38] Information Commissioner's Office, 'Right of Access', accessed 5 June 2018.
[39] Information Commissioner's Office, 'Right to Rectification', accessed 5 June 2018.
[40] Information Commissioner's Office, 'Right to Erasure', accessed 5 June 2018.
[41] Information Commissioner's Office, 'Right to Restrict Processing', accessed 5 June 2018.
[42] Information Commissioner's Office, 'Right to Data Portability', accessed 5 June 2018.
[43] Information Commissioner's Office, 'Right to Object', accessed 5 June 2018.

circumstances.[44]

The GDPR is directly applicable EU legislation, therefore for as long as the UK remains part of the EU it applies in the UK without the need for further legislation. Under the terms of the European Union (Withdrawal) Bill, all existing EU legislation, including the GDPR, will be preserved in UK law so that "as a general rule, the same rules and laws will apply on the day after the UK leaves the EU as before".[45]

In May 2018, Parliament passed related domestic legislation, in the form of the Data Protection Act 2018. This Act exercises certain available derogations in the GDPR, implements related EU data protection legislation and legislates in areas outside the EU's competence.[46] The Data Protection Act 2018 also includes provisions in relation to the role of the Information Commissioner.

3.3 Data Protection Act 2018: Powers of the Information Commissioner

The GDPR provides that each country should have a "supervisory authority", an independent public authority responsible for monitoring the application of the GDPR.[47] In the UK this function is undertaken by the Information Commissioner. In addition to the functions for the supervisory authority set out in the GDPR, the Data Protection Act 2018 outlines further rights and responsibilities of the Information Commissioner.

In the Data Protection Bill [HL], as introduced, the Information Commissioner was given the power to issue notices requiring data controllers or processors to provide them with information.[48] Failure to comply with such a request could result in the data controller or processor being subject to a fine.[49] During the passage of the Bill through Parliament, the Information Commissioner stated her view that the office of the Information Commissioner required more powers to obtain information than were provided for in the Bill as introduced. A briefing published by the Information Commissioner ahead of the Bill's second reading in the House of Commons, in March 2018, stated that one of the Information Commissioner's "most significant concerns" about the Bill related to "the Commissioner's ability to acquire the information she needs to assess whether the law has been broken".[50]

---

[44] Information Commissioner's Office, 'Rights Related to Automated Decision Making Including Profiling', accessed 5 June 2018.
[45] Explanatory Notes to the European Union (Withdrawal) Bill, p 8.
[46] Information Commissioner's Office, 'Data Protection Act 2018', accessed 6 June 2018.
[47] Regulation (EU) 2016/679, Article 51(1).
[48] Data Protection Bill [HL] (as introduced), clause 137.
[49] ibid, clause 148.
[50] Information Commissioner's Office, *Data Protection Bill, House of Commons Second Reading—Information Commissioner's Briefing*, March 2018, p 2.

The briefing continued:

> The Commissioner would like the Bill amended to provide a mechanism to require the disclosure of requested information under her Information Notice powers. Failure to do this will have an adverse effect on her investigatory and enforcement powers. The lack of such a mechanism at present is affecting her investigation of current significant cases.[51]

In evidence to the House of Commons Digital, Culture, Media and Sport Committee, Elizabeth Denham, the Information Commissioner, further explained why she felt these powers were necessary:

> In my parliamentary briefing on the Data Protection Bill, one of the deficiencies I see in terms of my powers is the ability to enforce an information notice. In the Data Protection Bill, I suggest to Parliament that I do not want a fine to be the result of an organisation refusing to co-operate with us. I actually want the information in an inquisitorial investigation. People should not be able to buy themselves out of compliance with our office's investigation.[52]

When the Bill was considered at report stage in the House of Commons, Margot James, Minister of State for the Department for Digital, Culture, Media and Sport, introduced a new clause, allowing the Commissioner to apply to the court for an order to force compliance when a person or organisation fails to comply with a requirement to provide her with information.[53] The Minister stated that as a result of this new clause, "organisations that might previously have been tempted to pay a fine for non-compliance instead of handing over the information will find themselves at risk of being in contempt of court if they do not comply".[54]

The Government also introduced at report stage amendments to allow the Commissioner to require any person who might have knowledge about suspected breaches of data protection legislation to provide information to the Information Commissioner; previously, information could be sought only from a data controller or a data processor.[55] This change was also requested by the Information Commissioner in her briefing.[56]

---

[51] Information Commissioner's Office, *Data Protection Bill, House of Commons Second Reading—Information Commissioner's Briefing*, March 2018, p 2.
[52] House of Commons Digital, Culture, Media and Sport Committee, *Oral Evidence: Fake News*, 6 March 2018, HC 363 of session 2017–19, Q901.
[53] HC *Hansard*, 9 May 2018, col 755.
[54] ibid.
[55] ibid.
[56] Information Commissioner's Office, *Data Protection Bill, House of Commons Second Reading—Information Commissioner's Briefing*, March 2018, p 3.

These changes were agreed without division, and are included in the Data Protection Act 2018. Section 145 deals with the court's powers to issue information orders, and section 142(1) states that the Information Commissioner can request information from people who are not data controllers or processors, under certain circumstances.

3.4 Special Categories of Data

The GDPR provides extra protection for special categories of data, which covers:

> […] 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.[57]

The GDPR prohibits processing of this type of data unless certain conditions apply:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;

[57] Regulation (EU) 2016/679, Article 9(1).

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[58]

The Data Protection Act 2018 adds more specific conditions to the processing of this type of data. Part 1 of schedule 1 of the Act defines the conditions under which processing meets the requirement in points (b), (h), (i) or (j) above. Schedule 1 part 2 contains specific substantial public interest conditions that must be met in order to rely on sub-section (h).

[58] Regulation (EU) 2016/679, Article 9(2).