Data Protection Bill

What is in this for local councils?

Local councils will wish to be aware of the Data Protection Bill which was announced in the Queen's Speech on 21 June 2017 and is currently progressing through the House of Lords. The formality of the First Reading was on 13 September 2017 and the Second Reading took place on 10 October 2017. This Bill comes under the remit of the Department for Digital, Culture, Media and Sport.

Local councils will be used to the terminology of the existing Data Protection Act 1998 in applying rules to them as data "controllers" and "processors". These rules will be extended under the new Bill and related EU legislation. The Bill is important for local councils as it seeks to empower individuals with rights to access and control their own data, along with having a right to be forgotten. The intention is that the emerging legislation will fundamentally shift the way local councils and other organisations deal with data through requiring fair, appropriate and lawful data management built into all their processes.

The current 1998 Act implemented the European Data Protection Directive (Directive 95/46/EC). On 25 May 2018 the Directive will be replaced when the General Data Protection Regulation (the GDPR) applies. Although the GDPR has direct effect in the UK without the need for implementing legislation, there are important reasons stated for the UK progressing its own Bill:

- **Gap-filling** - The Bill takes advantage of the GDPR leaving some limited opportunities to gap-fill and make detailed provision for particular aspects of the law.
- **Brexit** - Implementing new data protection controls in line with the GDPR will facilitate continued data transfer with the EU post Brexit.
- **Extension** - The Bill, ostensibly, rationalises application and legislation by also accommodating matters not covered by the GDPR, such as national security.
- **Modernisation** - The opportunity is taken to change the data protection framework in light of the increasing levels of digital personal data processing in an international environment and the pressure to give people more control over use of their data than currently available.

This LAIS focuses on the Data Protection Bill which is likely to change as it passes through the parliamentary processes. It is not possible just to look solely at the wording of the Bill when considering the intended applicable law, as cross-references are made to the GDPR throughout the body of the Bill.

This LAIS contains information condensed from a much larger body of information and only contains key points. Although every care is taken to ensure its accuracy, it should not replace a reading of the original text and guidance from the Information Commissioner. Only the courts can definitively interpret legislation and, additionally, the content of the Bill and the understanding of the Bill will evolve as the Bill progresses through Parliament. The length of this LAIS has been contained as far as reasonably possible without compromising content and some of the main points for local councils are highlighted within the text.

Date: The main parts affecting local councils (the GDPR) come in to effect on 25 May 2018. The law also gives effect to the Law Enforcement Directive and this element comes into effect on 6 May 2018. To enable Government to progress implementing secondary legislation, relevant regulation-making powers come into force on Royal Assent as do a limited number of clauses, as indicated within the text below.
References to local councils: Data Protection Bill: 1; GDPR: 0
Pages: Data Protection Bill: 21; Explanatory Note: 112; GDPR: 88.

Introduction

The Bill applies to data processing of 'personal data' in three situations: general data processing, which accounts for the vast majority of data processing across all sectors of the economy and the public sector; law enforcement data processing, which covers investigation of crime and the operation of the criminal justice system and the related rights of victims, witnesses and suspects; and intelligence services data processing by the three intelligence agencies dealing with national security.

The Bill and the General Data Protection Regulation (GDPR) provide new rights, many of which have been highlighted by the media, including rights of data subjects (individuals) to access their data, be forgotten and move their data to other places (portability). Affirmative consent becomes required for data processing (e.g. no pre-ticked boxes conferring consent).

For every right created for individuals, there are obligations imposed on organisations collecting, holding and processing data. This includes public bodies, such as local councils, which not only have to take extra measures to collect and safeguard data lawfully but must also appoint a suitable Data Protection Officer within or external to the council.

Additional enforcement powers and fines have been created. If a data breach risks the rights and freedoms of an individual, data controllers are required to notify the Information Commissioner within 72 hours of the breach taking place. In cases where there is a high risk, the individuals concerned must also be notified. There are a range of new offences, such as unlawful re-identification of de-identified personal data and altering or destroying personal data to prevent individuals accessing them.

Although mandatory provisions in the GDPR apply, there is controversy that some of the optional provisions have not been carried across to the Bill and that other provisions have been implemented inappropriately. As the Bill brings in additional data protection provisions not covered by the GDPR, the limited scope has also been the subject of criticism. At the Second Reading of the Bill some of the concerns raised include:

- A desire for stronger offences for unlawfully obtaining disclosure of personal data e.g. through 'blagging' information.
- The low age of consent for children – 13 years old.
- The degree of burden of consent provisions in the context of worthy not-for-profits and charities supporting, for example, vulnerable people.
- Lack of clarity about when the NHS and research establishments can use the 'public interest' provisions as a legal basis for processing data.
- The fact that many amendments are being made through secondary legislation which will not be subject to parliamentary scrutiny.
- The omission of the right of civil groups to take action on behalf of individuals without the need for the individual to take action themselves.
- Lack of clarity about when it is permissible to refuse access to data.
- How to secure the right balance between protecting freedoms and civil liberties while protecting a democratic society from various threats to safety and well-being.
- Concerns about stifling the free press through the inclusion of investigative journalism alongside a wide definition of 'personal data'.
- Insufficient control of 'fake news'.
- The plurality of regimes causing confusion and a lack of level playing field.
- The confusion caused by a complex new regime given that full guidance will not be available until next year, potentially as late as spring. This apparently owing to the fact that the Information Commissioner cannot issue their guidance until the European Data Protection Board guidance is issued.
- Fine levels being overly burdensome which might lead to cover-ups and feed the compensation culture.

- The claimed high cost of compliance. This will be on the minds of local councils. While concerns about additional funding from the public purse will be raised, there is an ongoing discussion with Government about whether new burdens funding should be made available to local councils given, potentially, costs linked to provision of an internal or external Data Protection Officer (additional hours or contract payments) and new data management system costs (encryption, security, storage etc) which will have to be considered.
- The complexity of the Bill, the cross-referencing to the GDPR and the fact that the GDPR will only be incorporated into domestic law post Brexit under the withdrawal Bill, with resultant difficulty for any organisation seeking to comply and any individual trying to work out what their rights will be:
  "…thinking about this Bill makes my head hurt" - Lord Knight of Weymouth.
  "Is the consequent cross-referencing to an absent document the best that can be done?" - Baroness Ludford
  "…I found this Bill incredibly hard to read and even harder to understand... we are sleepwalking into a dystopian future if we do not work hard to simplify the Bill and make it accessible to more people… from any perspective, the GDPR is difficult to comprehend, comprising sweeping regulations with 99 articles and 173 recitals. The Bill contains some wonderful provisions, of which my favourite is:
  "Chapter 2 of this Part applies for the purposes of the applied GDPR as it applies for the purposes of the GDPR … In this Chapter, "the applied Chapter 2" means Chapter 2 of this Part as applied by this Chapter"." - Baroness Lane-Fox of Soho.
- The difficulties in applying the Bill and GDPR to small local councils and the need for proportionality in approach.
  "My Lords, I very much agreed with those who said that the regulation must certainly apply to the big boys in the computer and digital world. I shuddered when the noble Baroness, Lady Lane-Fox, quoted from that wholly incomprehensible Brussels jargon from the regulations. I received last week a letter as chair of Marlesford Parish Council.
  "*We have seven members and only 230 people live in Marlesford. Our precept is only £1,000 a year. A letter from the National Association of Local Councils warned me that the GDPR will impose, "a legal obligation to appoint a Digital Protection Officer … this appointment may not be as straightforward as you may be assuming, as while it may be possible to appoint an existing member of staff"— we have no staff, just a part-time parish clerk who is basically a volunteer. It continues:*
  'They must by requirement of regulations possess 'expert knowledge of data protection law and practices'."
  I am afraid that will not be found in most small villages in the country, so I hope that one result of this Bill will be to introduce an element of proportionality in how it is to apply, otherwise the noble Baroness, Lady Lane-Fox, who was so right to draw our attention to the threat of incomprehensibility, will be right and we will all lose the plot."

The next stage for the Bill is Committee Stage due to start on 30 October 2017.

Meanwhile the Department for Digital, Culture, Media and Sport has written to the National Association of Local Councils (21 September 2017) stating:

- That parish councils and parish meetings will count as public authorities under the new data protection rules and therefore, all local councils will need to appoint a Data Protection Officer.
- Local councils can decide who should be their DPO. DCMS state that there is "considerable flexibility as to how this requirement is met." "It is a matter for each public authority to determine who should act as the DPO and what level of knowledge and expertise they require as they have the best knowledge of the personal data they process, any risks involved and the wider context in which they operate."
- Importantly, the clerk can be the DPO. However, local councils should note: "In order to avoid a conflict of interest a DPO should not determine the purpose or manner of processing personal data. Provided that a parish council is satisfied that a clerk does not do this then they could act as the DPO."

- Alternatively, an external DPO may be appointed and "Various options exist including sharing a person between parish councils or sharing with the district council or other principal local authority."
- As well as promising guidance is being prepared by the Information Commissioner, Government "is also considering what further support we can offer". The communication contains insistence that the regime will be proportionate and flexible.
- There is no indication that any type of council will be exempt from the provisions and the communication (signed off by the Deputy Director for the Data Protection Bill) ends on the line "I hope that we can continue to work together to help small local councils comply with the new law."

Councils will be among those concerned about the lack of guidance and information on the interpretation of the new rules and on how to proportionately and practically implement them. Work continues by Local Associations and the National Association of Local Councils to obtain further clarity. In the meantime, Local Associations will continue to provide support and information when opportunities arise.

Summary of main clauses

What follows is a summary of the main clauses of the Data Protection Bill at Second Reading.

PART 1 PRELIMINARY

Clause 1 Overview
States that the Act makes "provision about the processing of personal data", most of which will be subject to the GDPR. Comes into effect on Royal Assent.

Clause 2 Terms relating to the processing of personal data
This is a crucial section which helps define the application of much of the Bill. Important definitions include:
""The GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)."
""Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(b))." Councils need to consider this broad definition which might include pseudonyms attributable to individuals.
""Processing", in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as— (a) collection, recording, organisation, structuring or storage, (b) adaptation or alteration, (c) retrieval, consultation or use, (d) disclosure by transmission, dissemination or otherwise making available, (e) alignment or combination, or (f) restriction, erasure or destruction, (subject to subsection (14)(b) and sections 4(7), 27(2) and 80(3), which make provision about references to processing in the different Parts of this Act)."
""Filing system" means any structured set of personal data which is accessible according to specific criteria, whether

The GDPR has direct application. Article 5 sets out the data protection principles which constitute the main responsibilities for organisations, including local councils, which in summary are:
1. Personal data shall be:
(a) processed **lawfully, fairly and in a transparent manner** in relation to the data subject;
(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**; 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;
e) kept **in a form which permits identification of data subjects for no longer than is necessary**;
(f) processed so as to **ensure appropriate security of the personal data**, including against unauthorised or unlawful processing and against accidental loss, destruction or damage. There is some special provision, including for public interest archiving and historical research.

held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis." *Councils need to consider application of this legislation to their electronic and manual filing systems.*

This clause comes into effect on Royal Assent.

PART 2 GENERAL PROCESSING

CHAPTER 1 SCOPE AND DEFINITIONS

Clause 3 Processing to which this Part applies
States that Chapter 2 below relates to processing to which the GDPR applies whereas Chapter 3 covers certain other types of processing.
The Information Commissioner's Office advise that *you should assume that if you hold information that falls within the scope of the current Data Protection Act 1998, it will also fall within the scope of the GDPR*.

Clause 4 Definitions
GDPR definitions apply for the purposes of Chapters 2 and 3.

CHAPTER 2 THE GDPR

Meaning of certain terms used in the GDPR
Clause 5 Meaning of "controller"
Article 4 (7) of the GDPR defines 'controller' as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". Where obligations to process data arise in law the person required to process that data will be classed as the data controller.
Clause 6 Meaning of "public authority" and "public body"
These are not defined in the GDPR but essentially the definition is as per the Data Protection Act 1998 i.e. as defined by the Freedom of Information Act 2000.
So, as things stand the Bill applies to town and parish councils.

Lawfulness of processing
Clause 7 Lawfulness of processing: public interest etc
Processing of personal data is lawful where necessary for the performance of tasks conducted in the public interest or in the exercise of official

Local council processing of personal data must be lawful. Article 6(1) of the GDPR defines the lawfulness as including processing:

(a) With consent of the data subject
(b) Necessary for entering or performing contracts
(c) Necessary for compliance with a legal obligation
(d) Necessary for vital interests of the data subject or others
(e) Necessary for tasks in the public interest or for tasks under official authority

Article 6(1)(a) provides the most likely mechanism for ensuring the lawfulness of much of local council processing – prior consent.

Follow the Information Commissioner's advice:
Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.
Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data.
You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

authority vested in the controller. *Councils will wish to ensure that they are not unnecessarily holding and using personal data.*

Clause 8 Child's consent in relation to information society services

The Bill sets the age at which a child can consent to the processing of their personal data by most online services, as 13 years old. This would include services such as Facebook, online banking and websites buying and selling services. The GDPR does not permit a lower age to be used.

Special categories of personal data

Clause 9 Special categories of personal data and criminal convictions etc data

Under Article 9 of the GDPR it is generally prohibited to process special categories of personal data, such as those 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 purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This prohibition does not apply to certain matters e.g. for substantial public interest and public health, where processing is permitted subject to fulfilling special conditions (Schedule 1).

Clause 10 Special categories of personal data etc: supplementary

Supplementary provisions in connection with Clause 9.

Rights of the data subject

Clause 11 Limits on fees that may be charged by controllers

This part will be important for councils in relation to budgets and managing vexatious and unreasonable requests. Regulations may be made to specify limits on fees that may be charged in relation to "manifestly unfounded or excessive requests" or for the provision of further information.

Clause 12 Obligations of credit reference agencies

This provides specific provisions for credit reference agencies.

Clause 13 Automated decision-making authorised by law: safeguards

Interestingly this provides the right for individuals not to be subject to decision-making which is based solely on automated processes, including profiling, unless there is explicit consent, authorisation in law and safeguards, and it is a necessary process for contract creation. "Automated decision-making' is not defined.

Restrictions on data subject's rights

Clause 14 Exemptions etc

Provides for certain exemptions as set out in Schedules 2, 3 and 4 to deal with matters relating to specific matters such as health, "substantial public interest", criminal convictions and child abuse. National security and defence have specific provisions under Chapter 3 and clause 24.

Clause 15 Power to make further exemptions etc by regulations

Provides for regulations to make further exemptions.

Accreditation of certification providers

Clause 16 Accreditation of certification providers

Provides for a regulatory framework for accrediting bodies who can issue certificates to organisations demonstrating compliance with data processing requirements.

Transfers of personal data to third countries etc

Clause 17 Transfers of personal data to third countries etc

Provides for regulations restricting or enabling data transfers with a third country (non-EU or non-EEA) or international organisations where necessary for public interest reasons.

Specific processing situations

Clause 18 Processing for archiving, research and statistical purposes: safeguards

Data processing is subjected to restrictions and prohibitions designed to prevent use for decisions about subjects or where it "causes substantial damage or distress".

CHAPTER 3 OTHER GENERAL PROCESSING

Scope

Clause 19 Processing to which this Chapter applies

Chapter 3 applies the GDPR to "automated or structured processing of personal data" (fully or semi-automatic processing) which are outside of the scope of the GDPR and to certain common foreign and security policy activities. Law enforcement and national security are covered separately in Parts 3 and 4. Importantly this Chapter also covers unstructured manual data processing (i.e. non-automated or structured personal data) by a "public authority" for the purpose of the Freedom of Information Act (*includes local councils*).

Application of the GDPR

Clause 20 Application of the GDPR to processing to which this Chapter applies

This essentially says that data processing under this part shall be dealt with similarly to processing under the GDPR.

Clause 21 Power to make provision in consequence of regulations related to the GDPR

A power to make modifications to regulations.

Exemptions etc

Clause 22 Manual unstructured data held by FOI public authorities

This clause ensures that rights and duties not relevant to unstructured manual records e.g. data portability, are not applied. It also provides safeguards such as ensuring access rights are restricted in relation to the armed forces, the Crown and Government Department personnel matters.

Local councils will be familiar with the concept in Clause 22(5) where requests can be refused because they do not contain a description of the personal data or the controller estimates the cost of complying with the request for personal data would exceed the appropriate maximum. Normally the controller would still have to say whether or not the data is being processed.

Clause 23 Manual unstructured data used in longstanding historical research

Essentially this data is not subject to certain GDPR provisions where it was processed historically as long as certain conditions apply.

Clause 24 National security and defence exemption

Clause 25 National security: certificate

Clause 26 National security and defence: modifications to Articles 9 and 32 of the applied GDPR

Certain processing for national security and defence safeguarding is not covered by the applied GDPR scheme. This can be certified by a Minister of the Crown.

PART 3 LAW ENFORCEMENT PROCESSING

CHAPTER 1 SCOPE AND DEFINITIONS

Scope

Clause 27 Processing to which this Part applies Definitions

Clause 28 Meaning of "competent authority"

Clause 29 "The law enforcement purposes"

Clause 30 Meaning of "controller" and "processor"

Clause 31 Other definitions

The GDPR does not apply to the processing of personal data by competent authorities such as the police. Instead the Law Enforcement Directive (EU) 2016/6802 applies. This Law Enforcement Directive ("LED") is not directly applicable EU law; accordingly, Part 3 and relevant provisions in Parts 5 to 7 transpose the LED into UK law.

CHAPTER 2 PRINCIPLES

Clause 32 Overview and general duty of controller

Gives an overview of the data protection principles in relation to law enforcement, outlined in the next 6 clauses and states at 32(3) that "The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter" e.g. with the principles.

Clause 33 The first data protection principle

"the processing of personal data for any of the law enforcement purposes must be lawful and fair" and according to conditions.

The conditions include that the data subject has given permission or that "the processing is necessary for the performance of a task carried out for that purpose by a competent authority." There is no requirement to be "transparent" in relation to the data subject. This change ensures that enforcement authorities do not have to confirm or deny that they hold data. The wording is designed to continue to permit covert investigations and surveillance remain possible.

"Sensitive processing" is permitted for law enforcement where the subject consents or for a Schedule 8 reason and a policy must be in place (see Clause 40).

Clause 34 The second data protection principle

"(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and
(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected."

Clause 35 The third data protection principle

"personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."

Guidance on interpretation is provided by the Information Commissioner.

Clause 36 The fourth data protection principle

"(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and
(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay."

Clause 37 The fifth data protection principle

"personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed."

The lack of definition of the time limits might cause some problems, although there are some pre-existing legal specifications e.g. where persons are convicted of recordable offences, fingerprints and DNA profile may be kept indefinitely.

Clause 38 The sixth data protection principle

"personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

Guidance on interpretation is provided by the Information Commissioner.

Clause 39 Safeguards: archiving

Where processing for law enforcement purposes is necessary for archiving in the public interest, for scientific or historical research or for statistical purposes it must not be used for decisions about a data subject or cause substantial damage or distress to an individual.

Clause 40 Safeguards: sensitive processing
An appropriate policy is required for sensitive processing.

CHAPTER 3 RIGHTS OF THE DATA SUBJECT

Overview and scope
Clause 41 Overview and scope
Chapter 3 relates only to processing for law enforcement purposes and imposes general duties on controllers (as defined within Clause 5 above), confers rights on data subjects, regulates automated decision-making and makes supplementary provisions. Clauses 42 to 46 do not apply to the processing of relevant personal data for criminal investigations and proceedings.

Information: controller's general duties
Clause 42 Information: controller's general duties
Controllers are required to make available, as a minimum, the following information:
(a) the identity and the contact details of the controller;
(b) where applicable, the contact details of the data protection officer;
(c) the purposes for which the controller processes personal data;
(d) the existence of the rights of data subjects to request from the controller—
(i) access to personal data,
(ii) rectification of personal data, and
(iii) erasure of personal data or the restriction of its processing;
(e) the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.
This information can be made generally available to the public or in any other way, through their websites or supporting literature. The Commissioner has published a code of practice on communicating privacy information to individuals.
Controllers must also provide certain information to the data subject to enable the exercise of their access rights. Such rights can be restricted in certain circumstances, such as when it might compromise a police investigation.

Data subject's right of access
Clause 43 Right of access by the data subject
Data subjects are entitled to request:
(a) confirmation as to whether or not personal data concerning him or her is being processed, and
(b) where that is the case, access to that personal data and further specified information.
Importantly, the further information includes:
(a) the purposes of and legal basis for the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);
(d) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;
(e) the existence of the data subject's rights to request from the controller—
(i) rectification of personal data, and
(ii) erasure of personal data or the restriction of its processing;
(f) the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner; and
(g) communication of the personal data undergoing processing and of any available information as to its origin.
Should data subjects request information it must be provided in writing without undue delay, and, generally, in any event before the end of one month. Although they may restrict data provision in some situations, including for national security or to prevent prejudice to a criminal investigation. If rights are restricted, they must inform

the data subject of this, with reasons and stating their options for recourse. There is the option to neither confirm nor deny in order to avoid prejudicing investigations.

Data subject's rights to rectification or erasure etc
Clause 44 Right to rectification
Clause 45 Right to erasure or restriction of processing
A great deal of publicity has attached to these rights. Generally, controllers must, on request by the data subject, rectify without undue delay inaccurate personal data or, in some cases, erase data. In some cases, such as where it is not possible to ascertain the accuracy of data, its use must be restricted.
Clause 46 Rights under section 44 or 45: supplementary
Where rectification or erasure are requested, the controller must inform the data subject in writing of whether their request has been granted and, if not, reasons for refusal and the redress available.
Compliance must take place without undue delay, and, generally, in any event before the end of one month.
Rights may be restricted in some situations, including for national security or to prevent prejudice to a criminal investigation. If rights are restricted, the data subject must be informed of this, with reasons, and stating the options for recourse. There is the option not to comply, in order to avoid prejudicing investigations.
Significantly, controllers must notify the competent authority (if any) from which the inaccurate data originated and must notify recipients who are also then obliged to similarly rectify, erase or restrict the data processing.

Automated individual decision-making
Clause 47 Right not to be subject to automated decision-making
A crucial part of the new data protections is that a **"**controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law" i.e. automated decisions which significantly affect or produce an adverse legal effect for the data subject. It is recognised that this is not a common practice in a law enforcement context.
Clause 48 Automated decision-making authorised by law: safeguards
Where controllers take significant decisions required or authorised by law, the data subject must be informed and has options to request the reconsideration of the decision or a new decision not based solely on automated processing and response measures and safeguards are built into the legislation.

Supplementary
Clause 49 Exercise of rights through the Commissioner
The Commissioner's intervention may be requested where data provision is restricted.
Clause 50 Form of provision of information etc
Information provided must be in a "concise, intelligible and easily accessible form, using clear and plain language". It may be provided in any form, including electronic, but in the same format as the request, where practicable. While the identity of the requester is being verified, any format may be used. Generally, the information must be provided free of charge.
Clause 51 Manifestly unfounded or excessive requests by the data subject
Special provisions relate to "manifestly unfounded or excessive" requests e.g. mere repeats of the substance of previous requests, when refusal or charges may be applied.
Clause 52 Meaning of "applicable time period"
The "applicable time period" for responses is a month, or longer if specified in regulations, beginning on the latest of: the day the request is received, the day on which the requested information is received by the controller, or the day of receipt of a fee where applicable.

CHAPTER 4 CONTROLLER AND PROCESSOR

Overview and scope
Clause 53 Overview and scope
Describes the content of the Chapter in relation to controllers and processors.

General obligations

Clause 54 General obligations of the controller

Requires that appropriate technical and organisational measures must be taken by controllers to ensure compliance with Part 3, including through policies and proportionate measures.

Clause 55 Data protection by design and default

The measures must be designed from the outset and during processing to implement data protection principles effectively and integrate safeguards. By default, only personal data necessary for a specific purpose must be processed. In particular, measures must ensure data is not made accessible to an infinite number of people without an individual's intervention.

Clause 56 Joint controllers

Joint controllers must designate contact point and must determine their arrangements for compliance between them**.**

Clause 57 Processors

Where controllers use processors, conditions apply and such processors must provide guarantees to implement appropriate technical and organisational measures that are sufficient to secure compliance and protection of rights.

Clause 58 Processing under the authority of the controller or processor

Processors must process data only on instruction from the controller or to comply with legal obligations.

Clause 59 Records of processing activities

Clause 60 Logging

Records, as specified, must be kept by the controller of all categories of data processing used. Logs must be kept by the controller (or their processor) of automated processing systems for collection, alteration, consultation, disclosure (including transfers), combination and erasure. This enables monitoring and audit.

Clause 61 Co-operation with the Commissioner

This is required, as requested by the Commissioner.

Clause 62 Data protection impact assessment

Impact assessments by controllers are required prior to any processing where there is a high risk to the rights and freedoms of individuals. Any such assessment must include:

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks; and

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Clause 63 Prior consultation with the Commissioner

This is required before a controller creates a filing system for personal data where the impact assessment determines that processing would create a high risk to rights and freedoms of individuals (in the absence of mitigation measures). The Commissioner must provide advice where it is believed an infringement would result.

Obligations relating to security

Clause 64 Security of processing

Controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data. The burden of measures required is higher for automated processing and must:

a) Prevent unauthorised processing or interference
b) Provide the precise identification of processing that occurs
c) Enable restoration of interrupted functions
d) Prevent corruption in the event of malfunction

Clause 65 Notification of a personal data breach to the Commissioner

Where controllers become aware of a personal data breach they must notify the Commissioner without undue delay, and, where feasible, not later than 72 hours after becoming aware of it. If later than 72 hours a reason for

the delay must be given. Breaches do not have to be notified if they are unlikely to risk rights and freedoms of individuals. Records must be kept of breaches, their effects and any remedial action taken. Processors must inform controllers without undue delay of breaches. Relevant third parties from other member states who transmitted or received the data must be informed of breaches.

Obligations relating to personal data breaches
Clause 66 Communication of a personal data breach to the data subject
Where high risk breaches occur, the data subject must also be informed so that they can take steps to protect themselves. This must be carried out as soon as possible and appropriate, by mass communication if applicable. Restrictions apply on the need to comply with this duty for national security and specified other reasons.

Data protection officers
Clause 67 Designation of a data protection officer
A Data Protection Officer (DPO) must be appointed by the controller, having regard to "the proposed officer's expert knowledge of data protection law and practice", and their ability to perform the required tasks. The contact for the DPO must be published and notified to the Commissioner.
It is possible for organisations to share a DPO.
In defining the level of expertise, the explanatory note to the Bill states:
"An individual designated as a DPO must have the appropriate skills and training for the role. The level of knowledge should be consummate to the types of data processing the controller carries out; some types of processing will require a more bespoke skill set than others, a DPO for the police, for example, will require significant knowledge of the numerous systems that are operated in policing and the legal context for them. Depending on the size and function of the organisation, the DPO could be part-time or full-time, or one DPO could be appointed to work on behalf of several controllers (police forces for example could have one DPO per region as opposed to one per force). Irrespectively, the DPO will need to be suitably senior and resourced to be able to undertake his or her duties."
Clause 68 Position of data protection officer
The DPO must be suitably independent, free from conflicts of interest and have sufficient resources and training for their role. The DPO must also report to the highest management level. A data subject has the right to contact them regarding processing of their personal data and the exercise of their rights.
Clause 69 Tasks of data protection officer
Their tasks must include at least the following:
(a) informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Part,
(b) providing advice on the carrying out of a data protection impact assessment and monitoring compliance in that respect
(c) co-operating with the Commissioner,
(d) acting as the contact point for the Commissioner,
(e) monitoring compliance with policies (including assigning responsibilities, raising awareness, training staff and conducting audits under those policies), and
(f) monitoring compliance by the controller with this Part.

CHAPTER 5 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC

Overview and interpretation
Clause 70 Overview and interpretation
Deals with the transfer of personal data to third countries or international organisations.

General principles for transfers
Clause 71 General principles for transfers of personal data
Prohibits such transfers unless they meet three main conditions:

1) The transfer is necessary for any of the law enforcement purposes.
2) It is based on an adequacy decision, or, failing that, on there being appropriate safeguards, or, failing both of those, on special circumstances.
3) the intended recipient is a relevant authority for this purpose or certain conditions are met

Clause 72 Transfers on the basis of an adequacy decision

Adequacy decisions, referred to above, are those where third countries or other relevant parties have been determined as having an adequate level of protection of personal data by the European Commission under the LED.

Clause 73 Transfers on the basis of appropriate safeguards

Where third countries or other relevant parties are not recognised as having adequate levels of protection, transfer of data to them is prohibited unless certain safeguards are met.

Clause 74 Transfers on the basis of special circumstances

Where third countries or other relevant parties are not recognised as having adequate levels of protection or appropriate safeguards, transfer of data to them is prohibited unless specified special circumstances apply e.g. for immediate and serious public security threats.

Transfers to particular recipients

Clause 75 Transfers of personal data to persons other than relevant authorities

The additional 4 conditions for transfers to persons other than relevant authorities are set out.

Subsequent transfers

Clause 76 Subsequent transfers

If data is transferred out of the country as envisaged above in this Chapter, the transferring controller must impose a condition that the data is not for onwards transfer to another third country etc.

CHAPTER 6 SUPPLEMENTARY

Clause 77 National security: certificates by the Minister

For certain data matters, a Minister may issue certificates certifying that restrictions on rights and duties are valid for national security reasons.

Clause 78 Special processing restrictions

Where additional national restrictions apply, such restrictions must also be applied where such personal data is shared with a recipient in another EU Member State or other relevant country

Clause 79 Reporting of infringements

Controllers must encourage the reporting of infringements e.g. by raising awareness of protections for employees who make reports.

PART 4 INTELLIGENCE SERVICES PROCESSING

CHAPTER 1 SCOPE AND DEFINITIONS

Scope

Clause 80 Processing to which this Part applies

Part 4 of the Bill applies exclusively to personal data controlled by an intelligence service (the Security Service, Secret Intelligence Service and Government Communications Headquarters). These are specialist services with specialist functions and this LAIS does not cover them in detail. Much of the information is not significantly dissimilar from that for law enforcement generally but takes into account the particularly sensitive nature and impact of this activity.

Definitions
Clause 81 Meaning of "controller" and "processor"
Clause 82 Other definitions

CHAPTER 2 PRINCIPLES

Overview
Clause 83 Overview
The particular tailored application of the principles is outlined, following broadly similar themes as elsewhere in the Bill and with further detail in Schedules 9 to 10.

The data protection principles
Clause 84 The first data protection principle
Clause 85 The second data protection principle
Clause 86 The third data protection principle
Clause 87 The fourth data protection principle
Clause 88 The fifth data protection principle
Clause 89 The sixth data protection principle

CHAPTER 3 RIGHTS OF THE DATA SUBJECT

Overview
Clause 90 Overview Rights
The particular tailored application of available rights is provided in this chapter, following broadly similar themes as elsewhere in the Bill.
Clause 91 Right to information
Clause 92 Right of access
Clause 93 Right of access: supplementary
Clause 94 Right not to be subject to automated decision-making
Clause 95 Right to intervene in automated decision-making
Clause 96 Right to information about decision-making
Clause 97 Right to object to processing
Clause 98 Rights to rectification and erasure

CHAPTER 4 CONTROLLER AND PROCESSOR

Overview
The particular tailored application of obligations on controllers and processors is provided in this chapter, following broadly similar themes as elsewhere in the Bill.
Clause 99 Overview General obligations
Clause 100 General obligations of the controller
Clause 101 Data protection by design
Clause 102 Joint controllers
Clause 103 Processors
Clause 104 Processing under the authority of the controller or processor

Obligations relating to security
Clause 105 Security of processing
Obligations relating to personal data breaches
Clause 106 Communication of a personal data breach

CHAPTER 5 TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM

Clause 107 Transfers of personal data outside the United Kingdom
Such transfers of personal data to countries outside the United Kingdom or to an international organisation may only take place where "necessary and proportionate" for the controller's statutory functions or for certain security services purposes.

CHAPTER 6 EXEMPTIONS

Clause 108 National security
Clause 109 National security: certificate
Clause 110 Other exemptions
Clause 111 Power to make further exemptions
National security, with appropriate exemption certificate, provides an exemption from data protection principles and data subject rights, among other things. Schedule 11 applies.

PART 5 THE INFORMATION COMMISSIONER

The Commissioner
Clause 112 The Information Commissioner General functions
Makes provision for the Commissioner's continued existence and appointment (Schedule 12).
Clause 113 General functions under the GDPR and safeguards
The Commissioner is the supervisory authority for the purpose of the GDPR and safeguards apply.
Clause 114 Other general functions
The role is extended including to monitoring the application of the LED.
Clause 115 Competence in relation to courts etc
The Commissioner cannot supervise courts, judges or tribunals processing data for judicial purposes.

International role
Clause 116 Co-operation and mutual assistance
This is required with other supervisory authorities and relevant bodies.
Clause 117 Inspection of personal data in accordance with international obligations
A broadened power to inspect personal data held in any automated or structured system where the inspection is necessary to discharge an international obligation.
Clause 118 Further international role
Requires the Commissioner to engage with third countries and international organisations

Codes of practice
Clause 119 Data-sharing code
Requires the Commissioner publish and review a data sharing and good practice code.
Clause 120 Direct marketing code
Requires the Commissioner publish and review a direct marketing and good practice code.
Clause 121 Approval of data-sharing and direct marketing codes
Such codes are subject to parliamentary approval.
Clause 122 Publication and review of data-sharing and direct marketing codes
Specifies processes for publishing and reviewing the codes.
Clause 123 Effect of data-sharing and direct marketing codes
Such codes are admissible in evidence in legal proceedings and must be referred to by the Commissioner when making relevant determinations.
Clause 124 Other codes of practice
Other good practice codes may be required of the Commissioner by Government.

Consensual audits

Clause 125 Consensual audits Information provided to the Commissioner

Permits compliance audits to be made with the consent of the data controller or processor.

Clause 126 Disclosure of information to the Commissioner

Disclosure of needed information to the Commissioner is not precluded by other legislation.

Clause 127 Confidentiality of information

Requires non-disclosure of confidential information by the current and past Commissioner and related staff and agents.

Clause 128 Guidance about privileged communications

The Commissioner must create guidance about how they will deal with privileged communications.

Fees

Clause 129 Fees for services

Unsurprisingly, fees may be charged for the services provided or requested by others. This is not permitted for services for data subjects or data protection officers

Clause 130 Manifestly unfounded or excessive requests by data subjects etc

However, fees may be charged where data subjects make "manifestly unfounded or excessive requests" e.g. where the request "merely repeats the substance of previous requests."

Clause 131 Guidance about fees

The Commissioner must produce guidance about their own fee charges.

Charges

Clause 132 Charges payable to the Commissioner by controllers

For local councils it is worth noting that regulations may require controllers to pay charges of an amount specified in the regulations to the Commissioner. In setting the charge the Secretary of State will take into account the desirability of offsetting the amount needed to fund the Commissioner's data protection and privacy and electronic communications regulatory functions.

Clause 133 Regulations under section 132: supplementary

Consultation must take place for the purposes of regulations under clause 132.

Reports etc

Clause 134 Reporting to Parliament

The Commissioner must report annually.

Clause 135 Publication by the Commissioner

The Commissioner decides the appropriate means of publication for required reports.

Clause 136 Notices from the Commissioner

Specifies procedures for the issuing of notices under this Bill.

PART 6 ENFORCEMENT Information notices

Clause 137 Information notices

Creates a power and related provisions to require controllers or processors to provide certain information to the Commissioner. A minimum of seven days applies even for urgent requests.

Clause 138 Information notices: restrictions

Restrictions on the ability to request information apply e.g. in relation to legally privileged information or, unless there is a particular type of justification, data being processed for journalistic, academic, artistic or literary purposes.

Clause 139 Failure to comply with an information notice

An offence is created for such failure. A due diligence defence is provided which the defendant would have to prove on the balance of probabilities. An offence is also created for intentionally or recklessly making a false statement in response to an information notice.

Assessment notices

Clause 140 Assessment notices

Empowers the Commissioner and specifies related matters for the issuing of assessment notices for an assessment of compliance by a controller or processor. Such assessment notices might, for example, require permission to be granted to the Commissioner to enter premises or observe processing or for documents to be provided to the Commissioner.

Clause 141 Assessment notices: restrictions

Certain restrictions limit assessment notices e.g. in relation to legally privileged material.

Enforcement notices

Clause 142 Enforcement notices

Empowers and creates related provisions for the Commissioner, among other things, to issue enforcement notices for controllers and processors to take steps or refrain from actions in relation to failure to comply with the GDPR, failings by monitoring and certification bodies, and failure of controllers to comply in respect of charges payable to the Commissioner. Further regulations may be made empowering additional enforcement notice actions.

Clause 143 Enforcement notices: supplementary

These include a need for the Commissioner, when deciding whether to give an enforcement notice to controllers and processors for failures in relation to the GDPR, to consider whether the failure has caused or is likely to cause any person damage or distress. Permitted inclusions within notices are far-reaching and can include such matters as banning all processing of personal data.

Provides additional powers

Clause 144 Enforcement notices: rectification and erasure of personal data etc

Where these are issued owing to a failure in relation to accuracy of data processing or failure to rectify, erase or restrict data processing in line with data subject rights, they may include requirements to rectify or erase any resultant conclusions based on inaccurate information and inform third parties who might have relied on such information.

Clause 145 Enforcement notices: restrictions

Genuine processing for literary, artistic, journalistic or academic purposes is protected from the scope of enforcement notices.

Clause 146 Enforcement notices: cancellation and variation

The Commissioner can take and a controller can request such action.

Powers of entry and inspection

Clause 147 Powers of entry and inspection

Schedule 15 covers such powers.

Penalties

Clause 148 Penalty notices

Covers circumstances in which the Commissioner can issue a written penalty notice requiring the controller or processor to pay the Commissioner a fine, for failure to comply with certain provisions of the GDPR or this Act or failure to comply with an assessment notice or an enforcement notice. Power to make further regulations on this subject are provided.

Clause 149 Penalty notices: restrictions

Certain restrictions on issuing such notices are applied including where there is genuine processing for literary, artistic, journalistic or academic purposes.

Clause 150 Maximum amount of penalty

The maximum penalties imposed are notable, and, in summary, are: in some cases, 20 million EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is

higher, and in other cases, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher.

Clause 151 Fixed penalties for non-compliance with charges regulations

The penalties must be published. The maximum fine is 150% of the highest charge payable.

Clause 152 Amount of penalties: supplementary

Related regulations may be introduced.

Guidance

Clause 153 Guidance about regulatory action

Such guidance on the exercise of regulatory actions by the Commissioner must be published by the Commissioner.

Appeals

Clause 154 Rights of appeal

Includes details of the five specific notices that can be appealed to the tribunal: (a) an information notice; (b) an assessment notice; (c) an enforcement notice; (d) a penalty notice; and (e) a penalty variation notice.

Clause 155 Determination of appeals

Includes provisions enabling determinations to be upheld, replaced or altered etc.

Complaints

Clause 156 Complaints by data subjects

Importantly, this provides for the right of data subjects to make complaints to the Commissioner about infringements in relation to their own data and details the requirements on the Commissioner e.g. to take "appropriate steps" and keep the complainant informed.

Clause 157 Orders to progress complaints

Data subjects can apply for an order from the tribunal if the Commissioner does not perform certain actions in relation to complaints.

Remedies in the court

Clause 158 Compliance orders

Gives a data subject the right to apply for a court order against a controller or processor if their rights have been infringed e.g. rights to access, portability, rectification and erasure.

Clause 159 Compensation for contravention of the GDPR

Provides a broadened right to claim compensation from processors and controllers for damage suffered as a result of an infringement of the GDPR.

Clause 160 Compensation for contravention of other data protection legislation

Provides a similar broadened right to claim compensation for infringements of other data protection legislation.

Offences relating to personal data

Clause 161 Unlawful obtaining etc of personal data

An offence is provided "for a person knowingly or recklessly—
(a) to obtain or disclose personal data without the consent of the controller,
(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.
Public interest, crime-prevention, reasonable belief of legal entitlement and other defence provisions are provided.

Clause 162 Re-identification of de-identified personal data

Provides an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data. Some defences are provided for public interest etc.

Clause 163 Alteration etc of personal data to prevent disclosure
Provides an offence for controllers and related persons to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive. Defences are provided.

The special purposes
Clause 164 The special purposes
Provides for Commissioner action where "special purposes" are claimed in proceedings. These purposes are: (a) the purposes of journalism; (b) academic purposes; (c) artistic purposes; and (d) literary purposes.
Clause 165 Provision of assistance in special purposes proceedings
In matters of "substantial public importance", assistance from the Commissioner may be requested which might include paying costs in proceedings and indemnifying against related costs, expenses or damages.
Clause 166 Staying special purposes proceedings
Proceedings must be stayed if special purposes are claimed by controllers or processors.

Jurisdiction of courts
Clause 167 Jurisdiction
In England, the county court and High court are the courts which have jurisdiction for relevant parts.

Definitions
Clause 168 Interpretation of Part 6
Provides some details of where meanings of some terms are to be found.

PART 7 SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act
Clause 169 Regulations and consultation
Comes into effect on Royal Assent. Gives jurisdiction to the county court and High Court in relation to certain provisions.

Changes to the Data Protection Convention
Clause 170 Power to reflect changes to the Data Protection Convention
Gives the Secretary of State powers in this respect.

Rights of the data subject
Clause 171 Prohibition of requirement to produce relevant records
Provides offences, generally, for employers/contractors/suppliers requiring the provision of certain records via subject access requests as a condition of their contracts.
Clause 172 Avoidance of certain contractual terms relating to health records
Such terms requiring the provision of health records obtained through subject access requests would cause a contract to be void.
Clause 173 Representation of data subjects
Makes some provision for bodies authorised to represent data subjects to do so e.g. to complain to the Information Commissioner on their behalf.
Clause 174 Data subject's rights and other prohibitions and restrictions
This is a significant provision, essentially giving rights under this Bill a special status which can only be restricted through exemptions under the Bill; not through any other law.

Offences

Clause 175 Penalties for offences

Some of the criminal offences in the Act are summary only e.g. alteration of personal data to prevent disclosure (clause 163) and on conviction, an unlimited fine could be imposed. Others can be tried summarily or on indictment e.g. unlawfully obtaining personal data (clause 161) and again could attract an unlimited fine.

Clause 176 Prosecution

Prosecutions can be brought by the Information Commissioner or by, or with the consent of the Director of Public Prosecutions.

Clause 177 Liability of directors etc

Directors and similar can be prosecuted as well as the corporate body where breaches occurred with the consent, connivance or negligence of that person.

Clause 178 Recordable offences

Makes special provision for records in relation to offenders arrested for recordable criminal offences who may have fingerprints and DNA samples taken.

Clause 179 Guidance about PACE codes of practice

The Police and Criminal Evidence Act 1984 imposes duties in relation to the gathering of evidence including interviewing suspects, and charging offender. This provision enables the amendment of related guidance in light of the Bill.

The Tribunal

Clause 180 Disclosure of information to the Tribunal

Disclosure of certain information for the purpose of a tribunal is permitted.

Clause 181 Proceedings in the First-tier Tribunal: contempt

A First-tier tribunal may certify an offence of contempt of proceedings to the Upper Tribunal.

Clause 182 Tribunal Procedure Rules Definitions

Provides for related rules to be made.

Clause 183 Meaning of "health professional" and "social work professional"

Comes into effect on Royal Assent. These definitions are needed in relation to permissions for such persons to process data in permitted circumstances under the Act.

Clause 184 Other definitions

Comes into effect on Royal Assent. Defines terms not defined elsewhere e.g. "'publish' means make available to the public or a section of the public".

Clause 185 Index of defined expressions

Comes into effect on Royal Assent. Lists where certain expressions such as 'controller' are defined.

Territorial application

Clause 186 Territorial application of this Act

This confirms that UK based activity by controllers and processors and defines the application including where, in summary, they are not established in the UK but process data for individuals in the UK in relation to activities related to the UK.

General

Clause 187 Children in Scotland

Makes provision in relation to the age of consent by children in Scotland for data processing.

Clause 188 Application to the Crown

Comes into effect on Royal Assent. The Crown is not exempt.

Clause 189 Application to Parliament

Comes into effect on Royal Assent. Parliament is not exempt.

Clause 190 Minor and consequential amendments

Provides for such amendments as specified in Schedule 18 and enables regulations to be made including to amend or repeal primary legislation by affirmative resolution and otherwise legislation by negative resolution.

Final

Clause 191 Commencement

See summary box on page 1.

Clause 192 Transitional provision

Comes into effect on Royal Assent to enable relevant regulations to be made to provide for the transition.

Clause 193 Extent

Comes into effect on Royal Assent and defines differences in territorial application in the UK.

Clause 194 Short title

Comes into effect on Royal Assent to entitle the resulting legislation the Data Protection Act 2017.

The following schedules are included:

Schedule 1 Special categories of personal data and criminal convictions etc data
Part 1 — Conditions relating to employment, health and research etc
Part 2 — Substantial public interest conditions
Part 3 — Additional conditions relating to criminal convictions etc
Part 4 — Appropriate policy document and additional safeguards
Schedule 2 Exemptions etc from the GDPR
Part 1 — Adaptations and restrictions based on Articles 6(3) and 23(1)
Part 2 — Restrictions based on Article 23(1): Restrictions of rules in Articles 13 to 21
Part 3 — Restriction based on Article 23(1): Protection of rights of others
Part 4 — Restrictions based on Article 23(1): Restrictions of rules in Articles 13 to 15
Part 5 — Exemptions etc based on Article 85(2) for reasons of freedom of expression and information
Part 6 — Derogations etc based on Article 89 for research, statistics and archiving
Schedule 3 Exemptions etc from the GDPR: health, social work, education and child abuse data Part 1 — GDPR provisions to be restricted: "the listed GDPR provisions"
Part 2 — Health data
Part 3 — Social work data
Part 4 — Education data
Part 5 — Child abuse data
Schedule 4 Exemptions etc from the GDPR: disclosure prohibited or restricted by an enactment Schedule 5 Accreditation of certification providers: reviews and appeals
Schedule 6 The applied GDPR and the applied Chapter 2
Part 1 — Modifications to the GDPR
Part 2 — Modifications to Chapter 2 of Part 2
Schedule 7 Competent authorities
Schedule 8 Conditions for sensitive processing under Part 3
Schedule 9 Conditions for processing under Part 4
Schedule 10 Conditions for sensitive processing under Part 4
Schedule 11 Other exemptions under Part 4
Schedule 12 The Information Commissioner
Schedule 13 Other general functions of the Commissioner
Schedule 14 Co-operation and mutual assistance Part 1 — Law Enforcement Directive Part 2 — Data Protection Convention
Schedule 15 Powers of entry and inspection
Schedule 16 Penalties
Schedule 17 Relevant records
Schedule 18 Minor and consequential amendments

References

General Data Protection Regulation - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC can be found at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Data Protection Bill can be found at https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf. Associated documents can be found at https://services.parliament.uk/bills/2017-19/dataprotection.html and factsheets on the Bill can be found at https://www.gov.uk/government/collections/data-protection-bill-2017

Explanatory Notes to the Data Protection Bill can be found at https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066en.pdf

GDPR guidance can be found at www.ico.org.uk

Privacy notices, transparency and control: A code of practice on communicating privacy information to individuals can be found at https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

Hansard reports on the Second reading (part 1 and 2) can be found at https://hansard.parliament.uk/lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL); and https://hansard.parliament.uk/Lords/2017-10-10/debates/A0271CAB-90BC-49BD-B284-664918EE70CA/DataProtectionBill(HL)