NALC Advice Note - Data Protection

This advice note was written by our in-house solicitors and last updated on 1 November 2018.

The information and commentary in the note do not constitute legal advice for any individual case or matter. For specific advice on your circumstances, we strongly encourage you to seek tailored legal advice.

Introduction

The Data Protection Act 2018 ("the 2018 Act") came into force on 25 May 2018. The 2018 Act gives effect in UK Law to the General Data Protection Regulation ("GDPR"). It provides the statutory framework for the use of computerised information (including microfiche, audio and visual systems) and also certain manual records about living identifiable individuals in the United Kingdom. Data Protection legislation does not prohibit disclosures of such information to third parties, but it regulates the circumstances in which they can be made. It gives enhanced "subject access rights" (see below) and creates a new category of "sensitive data". It also prohibits the transfer of personal data to countries which do not have an "adequate level of protection". Annex 1 summarises in table form the relevant GDPR requirements.

Definitions

The 2018 Act again creates its own definitions, which can be found in Annex Two below. The important definitions are:

- "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Data subject" means the identified or identifiable living individual to whom personal data relates.
- "Personal data" means any information relating to an identified or identifiable living individual.
- "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:
    - An identifier such as a name, an identification number, location data or an online identifier.
    - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- "Processing", in relation to information, means an operation or set of operations which is performed on information or on sets of information, such as:
    - Collection, recording, organisation, structuring or storage.
    - Adaptation or alteration.
    - Retrieval, consultation or use.
    - Disclosure by transmission, dissemination or otherwise making available.
    - Alignment or combination.
    - Restriction, erasure or destruction.
- "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Processing – The Six Principles

Those who decide how and why personal data is processed (data controllers) must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection legislation.

Anyone processing personal data must comply with the six enforceable principles of good practice. They say that personal data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The legislation requires that personal data be processed "fairly, lawfully and in a transparent manner". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject is also entitled to know the identity of the data controller and why information is, or is to be, processed.

"Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:

- Collection, recording, organisation, structuring or storage.
- Adaptation or alteration.
- Retrieval, consultation or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure or destruction.

Processing may only be carried out where one of the following conditions has been met:

- Consent — The individual has given clear and explicit consent for you to process their personal data for a specific purpose.
- Contract — The processing is necessary for a contract you have with the individual or because they have asked you to take specific steps before entering into a contract.
- Legal obligation — The processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests — The processing is necessary to protect someone's life.
- Public task — The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. It is not enough to simply say: 'We have a legitimate interest in processing allotment holder data', as this does not clarify your purpose or intended outcome. Instead, you need to be more specific about your purpose, such as: 'We have a legitimate interest in ensuring that the allotments are used with the terms of the tenancy and the council's allotment rules".

In our opinion, local councils will be able to rely on several of these conditions in ensuring they comply with the 2018 Act.

Sensitive personal data is 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.

Sensitive data can only be processed where:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
- 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.
- 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.
- 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.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, for medical diagnosis, the provision of health or social care or treatment or for the management of health or social care systems and services.
- Processing is necessary for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices,
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Paper files/manual records

GDPR applies to "information kept on paper" if the paper records are kept within a "filing system." The term "filing system" is defined as "any *structured* set of personal data which [is] *accessible according to specific criteria*, whether centralised, decentralised or dispersed…" As a result, any files that "are not structured according to specific criteria" do not fall within the scope of the regulation.

Rights of data subjects

A person about whom information is held (a 'data subject') is, subject to any exemptions applying, entitled to:

- Be informed by any 'data controller' whether any information is held on them together with:
    - A description of the data.
    - aAcopy of the information in an intelligible form.

- Request and receive information giving:
    - The purposes for which the data is being held.
    - The recipients or classes of recipients to whom it may be disclosed.
    - The source of the data.
- Restrict the processing of their data.
- Object to the processing of personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing).
- Not to be subject to automated decision-making.
- Receive compensation from the data controller and/or the data processor for the damage suffered as a result of an infringement of GDPR.
- Obtain from a data controller without undue delay the rectification of inaccurate personal data.
- Erase personal data (also known as the "right to be forgotten"), which means that data subjects will be able to request that their personal data be erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with GDPR. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims. Where the data controller has made the personal data public and is obliged to erase the personal data, it shall take reasonable steps to inform data controllers who are processing the personal data that the data subject has requested them to erase any links to or copy or replication of that personal data.
- Be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights.
- Receive a copy of personal data or to transfer personal data to another data controller (data portability).

Access to personal data held by a data controller must be dealt with within one month of the request and free of charge. Where requests are manifestly unfounded or excessive, in particular, because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond.

Registration

Under GDPR, there is no requirement for a data controller to register with the ICO. However, the Data Protection (Charges and Information) Regulations 2018 ("the 2018 Regulations") require data controllers to pay a data protection fee to the Information Commissioner's Office ("ICO") unless they are exempt from payment. Councils in England and Wales and parish meetings are public authorities for the purposes of the 2018 Regulations and they are data controllers.

Data controllers with up to 10 members of staff will pay a fee of £40 (tier 1); data controllers with more than 10 members of staff but less than or 250 will pay £60 (tier 2); and data controllers with more than 250 members of staff will pay £2900 (tier 3).

Members of staff include employees, other workers and office holders. Each part-time staff member is counted as one member of staff.

Information Commissioner's Office - Data protection fee self-assessment

Non-payment or incorrect payment of the data protection fee could result in a fine of £4,350.

Councillors who are data controllers independent of their council (e.g. constituency casework or election canvassing) will be required to pay the data protection fee.

Exemptions

Data Protection legislation exemptions from obligations and individual rights include:

- National security.
- Defence.
- Public security.
- The prevention, investigation, detection or prosecution of criminal offences.
- Other important public interests, in particular, economic or financial interests, including budgetary and taxation matters, public health and security.
- The protection of judicial independence and proceedings.
- Breaches of ethics in regulated professions.
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention.
- The protection of the individual, or the rights and freedoms of others.
- The enforcement of civil law matters.

Also exempt are:

- Manual unstructured data held by public authorities, which includes local councils (e.g. loose pieces of paper not held in a structured format).
- Manual unstructured data used in longstanding historical research.

Penalties

If the ICO is satisfied that a data controller has breached the legislation, it is open to that Office to serve an enforcement notice requiring compliance. Failure to comply with such a notice can be a criminal offence punishable with a fine.

In addition, the court and ICO have power to award compensation to data subjects who suffer damage and distress as a result of any contravention by a data controller of any of the requirements of the 2018 Act.

How does the 2018 Act affect local councils?

Whilst there are exemptions to the requirements and individual rights. NALC takes the view that local councils will be hard-pressed to argue that all their data processing falls within the scope of those exemptions. In short this is because local councils (like all local authorities) hold such a wide range of information.

It is clear that councils are affected by the provisions of the Data Protection legislation in a multitude of ways. “Personal data” may be as simple as holding someone’s name and address but in addition includes amongst other things details of complaints, lists of contacts, employee/personnel records and information provided for the purpose of placing a contract to which the data subject is a party. Images taken by CCTV systems also fall within the data protection regime.

The following are a number of practical considerations which a council may wish to bear in mind to help ensure it complies with the 2018 Act:

- A council should first look at any data it holds to see if it includes personal data. Particular attention should be given to such things as contractor/supplier lists where there are businesses involved as

they could contain personal data as many businesses are owned by sole traders or partnerships. Even with companies, a council may store personal data on contacts at the company.

- It should be noted the legislation only applies to the "processing" of personal data but processing is so widely defined it will in fact catch almost any conceivable operation on such data.
- A council should (if appropriate) consider where it obtained any personal data from. Unless it can prove it was obtained fairly there is a risk the law will be broken. What constitutes "fairly" is somewhat complex but it includes the data subject consenting to the council using it e.g. was the data subject originally told their data might be given to third parties?
- A council should ensure that individuals are aware of the uses that will be made of the information they supply and, where necessary, give their consent to that specific use. Where there is a legitimate interest or a legal requirement then consent need not be explicitly obtained. Otherwise an explicit consent must be obtained.
- Data should never be given (or sold) to anyone else unless the data subject has given his/her consent or there is, by law, a duty to do so. Use of personal data on a website will automatically be a breach of the legislation unless express consent has been given e.g. publishing staff names and mobile numbers.
- A council obtaining consent to any use should make sure that it is "informed consent" i.e. that is been made very clear exactly what the council intends using the data for and what data it is holding.
- A council should ensure it only keeps the bare minimum amount of information necessary for its purposes. It should carry out regular reviews to check that all of the information asked for on for example as application forms or registration forms really is necessary.
- All data recorded must be accurate, kept up-to-date and deleted when no longer required.
- The information must be kept safe and secure at all times. The level of security will depend upon the sensitivity of the data involved. Listed below are some good practice points:

Manual records

25. Filing cabinets must be locked outside of normal working hours and keys must be held securely by nominated staff. It is advisable for more than one person to hold the keys e.g. clerk and another staff member of councillor. All papers should be securely locked away when not in use to prevent other people from inadvertently gaining access. Councils should have processes in place for homeworkers and information security.

Computerised records

The following guidelines apply:

- Access should be controlled by a unique password, and passwords should be changed on a regular basis. Passwords should not be obvious, e.g. 12345, password.
- Passwords and access controls should be kept secure when not in use e.g. passwords should not be written down and attached to PCs.
- Personal information should not be left displayed on the screen when not in use – councils should consider setting up screens to automatically lock after a certain period, e.g. four minutes.
- Removable devices such as USB sticks should be filed away securely and not left lying around.
- Computers should be turned off when not in use.
- If the personal data is held on a laptop or tablet these should be securely stored when not in use and be password protected.

- Workspaces containing a computer or other device containing data should be locked when not in use.

Further information

The regulatory body with responsibility for enforcing the legislation's requirements and promoting compliance and good practice is the ICO. The relevant contact details are:

- Address — Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
- Helpline — 0303 123 1113
- **Website** (includes live chat option)

The ICO provides advice and publishes useful guidance on data protection legislation. Councils can also contact the ICO with non-legal queries.

Annexe one — Subject and GDPR requirements

- Data protection principles
    - Personal data must be:
        - Processed fairly, lawfully and in a transparent manner in relation to the data subject.
        - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
        - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
        - Accurate and, where necessary, kept up to date.
        - Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
        - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5).
- Consent — Data controllers are required to have a legitimate reason(s) for processing personal data and where the data controller is relying on an individual's consent, the data controller must be able to demonstrate that consent by a statement or by a clear affirmative action, was freely given, specific, informed and unambiguous for each purpose that it is processed. Prior to giving consent, the individual shall be informed of his right to withdraw his consent at any time. In other words, it should be as easy to withdraw consent as to give it (Articles 4 and 7).
- Consent for children — Limits the ability of a child under 16 to consent to their personal data being processed in respect of "information society services", e.g. online businesses or social networking sites. This means that personal data is being processed for a child under 16. Consent must be obtained from the child's parent or custodian. An EU member state may lower the age at which a child can give consent to the processing of their data from 16 to 13. (Article 8). In the UK, children aged 13 years or older can consent to their personal data being processed for information society services.
- Privacy notices (also known as fair processing notices)
    - Information to be given by data controllers in privacy notices includes the following:

        - The identity and contact details of the data controller and, if any, of the controller's representative and of the data protection officer.
        - The purpose(s) of the processing.
        - The categories of personal data concerned.
        - The recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.
        - Where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period.
        - The right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
        - The right to lodge a complaint with the ICO.
        - Where the personal data is not collected from the data subject, any available information as to its source (Articles 13 and 14).
- Communications by data controllers — There are requirements on the data controller regarding the communications in a privacy notice and to the data subject relating to the rights of the data subject. Information provided must be in a concise and intelligible form using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing or by other means, including, where appropriate, electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means (Article 12).
- Data controllers working with data processors.
    - The data controller must enter into a contract with the data processor, which imposes the following obligations on the processor:
        - Process the personal data only on the documented instructions of the controller. This is likely to mean that data processors cannot use cloud computing technology or services without the data controller's approval.
        - Comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR.
        - Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality.
        - Enlist a sub-processor only with the prior permission of the controller.
        - Assist the controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR (including the right to transparency and information, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing).
        - Assist the data controller in carrying out its data security obligations under Articles 32 to 36 of the GDPR (Article 28).
- Privacy Impacts assessment (PIA) — Where a type of processing in particular uses new technologies and the purpose(s) that the data controller wishes to process personal data poses high risks, it will have to carry out a data protection privacy impact assessment before such processing (Article 35).

The ICO is expected to provide guidance about the type of processing that would demand a data protection privacy impact assessment.

- Notification by data controllers — Data controllers must maintain a written record of processing activities under their responsibility. The written record shall include a description of the categories of data subjects and the categories of personal data, purpose(s) of processing, categories of recipients of personal data, time limits for erasure and description of technical and organisational measures to protect data. Data processors also have a new duty to maintain a written record of similar information. However, the obligation to maintain a written record does not apply to an organisation employing less than 250 persons unless the processing it carries out is likely to result in risks to the rights of data subjects, the processing is not occasional, or the processing includes special categories of data e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or processing criminal convictions and offences. (Article 30).
- Appointment of Data Protection Officer (DPO) — Local councils are not obliged to appoint a DPO unless they process high volumes of sensitive personal data but they may appoint a DPO if they wish.
- Notification to report personal data breaches — Data controllers are required to report personal data breaches to the ICO without delay and within 72 hours. A data processor must also notify a data controller without undue delay after becoming aware of a personal data breach (Article 33).
- Fines — There are heavy fines for data controllers and data processors for a wide range of breaches. Some breaches (e.g. failing to comply with data subjects' rights or the principles for processing, including conditions for consent) attract fines of up to 4% of annual turnover for the preceding year or 20 million Euros, whichever is higher. For other breaches (e.g. failing to keep records of processing activities or to comply with security obligations), the fine can be up to 2% of annual turnover or 10 million Euros, whichever is higher (Article 83).
- Individuals' rights:
    - The right of access to personal data held by a data controller must be dealt with within one month of request and free of charge. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond (Articles 12 & 15).
    - The right to restriction of processing (Article 18).
    - The right to object to the processing of personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing) (Article 21).
    - The right not to be subject to automated decision-making (Article 22).
    - The right to receive compensation from the data controller is retained and there is a new right to receive compensation from the data processor for the damage suffered as a result of an infringement of GDPR (Article 82).
    - The right to obtain from a data controller without undue delay the rectification of inaccurate personal data (Article 16).
    - The right to erase personal data (also known as the "right to be forgotten") which means that data subjects will be able to request that their personal data be erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with GDPR. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims. Where the data controller has made the personal data public and is obliged to erase the personal data it

shall take reasonable steps to inform data controllers which are processing the personal data that the data subject has requested them to erase any links to, or copy or replication of that personal data (Article 17).

- A right to be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights (Article 34).
- A right to data portability - to receive a copy of personal data or to transfer personal data to another data controller (Article 20).

The above Articles are references to the relevant section of the EU General Data Processing Regulation.

Annexe two — Glossary of terms

- "Personal data" means any information relating to an identified or identifiable living individual.
- "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:
  - An identifier such as a name, an identification number, location data or an online identifier.
  - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:
  - Collection, recording, organisation, structuring or storage.
  - Adaptation or alteration.
  - Retrieval, consultation or use.
  - Disclosure by transmission, dissemination or otherwise making available.
  - Alignment or combination.
  - Restriction, erasure or destruction.
- "Data subject" means the identified or identifiable living individual to whom personal data relates.
- "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Processor" means a natural or legal person public authority, agency or other body which processes personal data on behalf of the controller.
- "Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- "Third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
- "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- “Filing system” means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.
- “The Commissioner” means the Information Commissioner.
- “The data protection legislation” means:
    - The General Data Protection Regulation.
    - The Data Protection Act 2018.
    - Regulations made under that Act.
    - Relevant regulations made under section 2(2) of the European Communities Act 1972.
- “Sensitive personal data” is 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.