the audience agency

Data Protection -

What the regulations say

Adam Kerr

Senior Partner, Primas Law

May 2018

Contents

1.1 Brief Introduction to the UK Data Protection Regime

1.2 Background

The Data Protection Act 1998 (the "DPA") implemented the EU *Directive 95/46/EEC* on the protection of individuals with regard to the processing of personal data and on the free movement of such data and replaced the UK's previous Data Protection Act 1984 in its entirety. The overarching purpose of the EU Data Directive was to introduce an extensive data protection regime by imposing broad obligations on those who collect personal data, as well as conferring broad rights on individuals about whom data is collected. The new General Data Protection Regulation (*679/2016/EU*) (GDPR) will replace the DPA and bring with it significant changes to the data protection framework within the European Union. The GDPR will be enforceable by the Information Commission in the UK as of 25 May 2018.

1.3 Brexit and GDPR

Given the timing of the UK's proposed separation from the EU, the GDPR will have already taken effect in the UK. However, at the time of the UK's exit from the European Union, the GDPR would cease to apply without UK legislation adopting the GDPR's provisions (the DPA would continue to apply because it is an act of Parliament). The prevailing view is that the UK will adopt the GDPR by way of domestic legislation so as to ensure consistency with the EU. That will enable data to continue to be sent between the UK and the EU in much the same way as was the case before Brexit. We await clearer guidance on the issue.

1.4 Key definitions

A brief review of some of the key terms used by the DPA is probably helpful:

Data Controller

The person who either alone, jointly or in common with other persons determines the purposes for which and the manner in which any personal data is, or is to be, processed. A party may be a data controller even if the information concerned is held by somebody else. There can also be more than one data controller in respect of a piece of data.

Most, if not all, of the principal obligations in the DPA fall on the data controller.

Data Processor

A data processor processes personal data only on behalf of a data controller.

Data Subject

An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal Data

Any information relating to a data subject.

Sensitive personal data, which attracts a high degree of protection, is data which is in relation to race, political opinions, health, sexual life, religious and other similar belief, trade union membership and/or criminal records.

1.5 The data protection principles

Following the introduction of the GDPR, seven data protection principles will apply. The seven principles require that:

1. personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (*Article 5(1)(a)*).
2. personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. (*Article 5(1)(b)*.)
3. personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (*Article 5(1)(c)*). The introduction

of a "necessity" requirement is likely to make it more difficult for data controllers to collect data for some general or as yet unspecified future use.

4. personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (*Article 5(1)(d)*).
5. personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (*Article 5(1)(e)*). Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.
6. personal data must be processed in a manner that ensures its appropriate security (*Article 5(1)(f)*). This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In this regard, data controllers and processors must use appropriate technical or organisational security measures.
7. the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles (*Article 5(2)*).

1.6 The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR")

The PECR are not relevant to all data protection matters but the Regulations do complement the DPA by giving more specific rights in respect of electronic communications.

The PECR principally cover the following areas:

- Marketing by electronic means, including marketing calls, texts, emails and faxes.
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service.

- Security of public electronic communications services.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

In relation to marketing, and in short, the PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic messages. The rules are generally stricter for marketing to individuals than for marketing to companies. Specific consent is required in order to send unsolicited direct marketing to someone.

2.1 Collecting Data

The act of obtaining data constitutes processing. As such, the obligations of the party collecting the data and the application of the GDPR's principles begin from the moment data processing and collecting activities are contemplated.

The point at which the data is obtained from the data subject (and even beforehand) is arguably the most important part of the data journey. This is because what is agreed with the data subject at the point of collection in relation to their data will largely (albeit not exclusively) govern what can and must happen to the data thereafter.

If you are collecting the data directly from the data subject, you must provide the following information to the individual at the time when you are collecting the information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- details of the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the legitimising condition for processing is the legitimate interests pursued by the controller or by a third party, the legitimate interests must be set out;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority, being the ICO;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The most common and effective way of providing the data subject with any or all the above information is by way of a privacy notice. All information provided to the data subject should be concise, transparent, intelligible and easily accessible, written in clear and plain language, particularly if addressed to a child.

3.1 Lawful Processing

There is a fundamental difference between (i) informing a data subject how you are going to use their data and, (ii) getting the data subject's consent to that use. The data controller must be able to justify the processing of the data in order for that processing to be considered lawful.

In order to be lawful, the processing must either:

- be as a result of consent given by the data subject to the processing of their personal data for one or more specific purposes; or
- be necessary for entering or performing a contract with the data subject; or
- be necessary for compliance with a legal obligation to which the data controller is subject; or
- be necessary to protect the vital interests of the data subject; or
- be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- be necessary for the purposes of legitimate interests pursued by the data controller, except where these interests are overridden by the interests for the fundamental rights and freedoms of the data subject which require the protection of personal data.

3.2 Legitimate interests basis

That final ground for lawful processing may at first appear applicable in a variety of situations. However, it should be treated with some caution. The guidance to the GDPR suggests that when assessing whether this ground can be relied upon, emphasis will be placed on what reasonable expectations the data subject had about how their data would be used, given the subject's relationship with the data controller. As such, the specifics of this ground should be carefully assessed in practice in order for the controller to be confident that it provides a solid basis for data processing activities. Privacy notices can obviously assist in the context of a data subject's reasonable expectations as to how their data will be used and processed.

If the data controller wants to use personal data it holds for a purpose which is different to the original purpose the data was collected for, that further processing must be justifiable on one of the above grounds; the data cannot simply be re-designated.

3.3 Consent

Obtaining consent from the data subject for the proposed processing is obviously the most unambiguous basis for lawful processing. Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

To qualify as consent, 'affirmative action' on the part of the data subject is required. That means that consent cannot be inferred from silence, pre-ticked boxes or inactivity by the data subject. A positive 'opt-in' is to be obtained.

Other key points to note in relation to consent:

- If consent is given in a written document, like a contract, that also concerns other matters, the consent element must be distinguished from the other matters.
- The data subject has the right to withdraw their consent at any time.
- When the processing has multiple purposes, consent should be given for all of them.

3.4 When should consent be obtained?

Consent should be obtained prior to any data processing unless any of the other legitimising grounds in the GDPR apply.

3.5 What constitutes valid consent?

Freely given consent

This has been taken to mean that:

- the data subject has a real choice about whether to consent to what the data controller wants to do with the data; and
- There is no risk of deception, intimidation, coercion or significant negative consequences if the data subject does not consent.

Specific consent

In order to be specific, consent must be given with respect to the type of personal data that is processed and the exact purpose for which it is processed. Different aspects of the processing must be clearly identified. Blanket consent for an open-ended set of processing activities is not sufficient. This means that the consent obtained must refer clearly and precisely to both the scope and the consequences of the data processing.

Informed Consent

The most effective way of ensuring that informed consent can be given by the data subject is for the data controller to express the information in a clear and understandable way. The information should also be readily accessible.

Unambiguous consent

In short, this means that the indication by which the data subject signifies their agreement to the data processing in question must leave no doubt about the fact that the data subject does, in fact, agree to that processing.

4.1 Data Sharing

It is worth noting from the outset that data sharing between parties is perfectly permissible, so long as such sharing is done in a proper, and GDPR compliant, fashion.

The sharing of data between two (or more) parties can either take the form of sharing between joint data controllers or between a data sharer and a data processor. Whilst each instance of sharing should be analysed on its own facts, in the context of sharing between venues and touring companies it is more likely than not that the venue will be the data controller and the touring company will be the data processor.

GDPR increases the obligations on both data controllers and processors when compared to the situation under the Data Protection Act.

In the first instance, an examination of the lawful basis for the processing is required (consent, legitimate interests and so on). Further processing of the data beyond that which was originally anticipated is only permitted as long as the new processing activity is not incompatible with that original purpose. So at the point of considering sharing data, an assessment will be required as to whether the sharing is within the original lawful basis for processing. The data controllers privacy notice should address the circumstances of any proposed or prospective sharing.

All of the data processing principles set out at article 5 of the GDPR very much apply to data sharing.

In addition, and in particular, the sharing of data between controller and processor requires the controller to enter into a written contract with the processor. Article 28 of the GDPR sets out what that contract must, as a minimum, contain. If the data controller employs more than 250 people, certain records must be kept in relation to the processing; although good practice and governance would suggest that organisation would be sensible to retain the records prescribed by article 30 whether it employs more than 250 staff or not.

It is also incumbent on the data controller to ensure the security of the data that it is passing on to the processor. This obligation requires the controller, in conjunction with the processor, to consider:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

When assessing the appropriate level of security, controllers and processors must take account of the risks presented by processing from (amongst other things) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

In order to assist in analysing the risks and benefits associated with data sharing, and as a matter of good practice and governance, data controllers would be well-advised to carry out privacy impact assessments in relation to the proposed sharing of data even if the GDPR does not specifically require such a privacy impact assessment to be undertaken in the circumstances.

5.1 Uses

As a general rule, personal data must be collected only for specified, explicit and legitimate purposes, and used in accordance with those agreed purposes. Save as detailed below, the data must not be further processed in any manner incompatible with the original purpose for which it is collected.

5.2 Research/statistical purposes exemption

In addition to the data being processed for the original purpose for which it was obtained, further processing is permitted for the following purposes:

- Archiving in the public interest;
- Scientific or historical research purposes;
- Statistical purposes.

It is important to note that reliance on the above exemption does not excuse the data controller from complying with its other obligations in respect of the data. More stringent conditions continue to apply if the data is sensitive personal data.

With regards the application of the research exemption, it is important to note that the scope of such permissible research is limited to that of a scientific or historical nature. Previous guidance under the Data Protection Act, which is considered to continue to apply here, suggests that further processing which is only for research purposes and which has not been expressly authorised by the data subject is not unlawful so long as the following two conditions are met:

- The data is not processed to support measures or decisions with respect to particular individuals; and
- The data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

6.1 Data Subject's Rights

The GDPR reaffirms some existing rights but also introduces some new ones. The full list of rights is as follows:

1. The right to be informed: Fair processing information must be provided to the data subject. The information to be provided depends on whether the information was obtained directly from the data subject or from a third party. Privacy notices are the usual way of complying with this obligation.
2. The right of access: Data subjects have the right to be told that their data is being processed and the right to access the information held about them. Such access should be given free of charge unless the request is excessive or unfounded.
3. The right to rectification: If data held about a subject is inaccurate, the data subject can ask to have it corrected. If the organisation has passed the incorrect data on to a third party, the organisation should rectify with the third party too where possible.
4. The right to erasure: See below.
5. The right to restrict processing: See below.
6. The right to data portability: This is a new right under GDPR. The data subject now has the right to receive a copy of their data back from the data controller in a commonly used electronic format for personal use on a private device. The data subject can also require their data to be transferred between data controllers.
7. The right to object: A data subject may object to processing for (i) For direct marketing purposes, including profiling related to direct marketing, (ii) For scientific or historical research purposes or statistical purposes unless the processing is necessary for the performance of a task carried out in the public interest, (iii) if the legitimising ground for the processing is based on the organisation's legitimate interests (or the performance of a task in the public interest/exercise of official authority). In those circumstances, the organisation must cease processing the data unless the data controller can demonstrate a compelling legitimate ground for processing the data that overrides the data subject's interests or the controller needs to process the personal data to establish, exercise, or defend legal claims.
8. Rights in relation to automated decision making and profiling: Data subjects have the right to not be subject to automated decision-making, including profiling, which has legal or other significant effects on the data subject. The right does not apply in the event that the automated decision is either (i) necessary for entering into or performing a contract with the data subject, (ii) authorized by law if that law requires suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, (iii) based on explicit data subject consent.

6.2 The right to erasure

Often referred to as the 'right to be forgotten', this right is often misunderstood. It is not an absolute right to be forgotten.

The right of erasure already exists under the DPA but is limited to processing that causes unwarranted and substantial damage or distress to the data subject. The criteria is not necessary for the right to be engaged under GDPR.

The data subject is entitled to the removal of their data (or to prevent further processing of the data) if:

- the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- the individual withdraws consent.
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed.
- the personal data has to be erased in order to comply with a legal obligation.
- the personal data is processed in relation to the offer of information society services to a child.

An organisation may refuse to comply with a request from a data subject if the data is required by the organisation:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

6.3 Right to object to processing

Data subjects may restrict the processing of their personal data:

- When the data subject contests the accuracy of the personal data in which case the data controller must restrict processing the contested data until it can verify its accuracy.
- If the processing is unlawful then instead of requesting erasure, the data subject can request that the data controller restricts the use of the unlawfully processed personal data.

- The data controller no longer needs to process the personal data but the data subject needs the personal data for the establishment, exercise, or defence of legal claims.
- The data subject objects to processing that relies on the public interest or the data controller's or a third party's legitimate interests as the lawful processing grounds. The data controller must restrict the challenged processing activity pending verification of whether the controller's legitimate interests override the data subject's interests.

7.1 Accountability

The GDPR requires a data controller to demonstrate that data processing activities comply with the GDPR's requirements.

Demonstrating compliance will require evidence of:

- Internal policies and processes that comply with the GDPR's requirements;
- The implementation of the policies and processes into an organisation's activities;
- Effective internal compliance measures;
- External controls.

The practical consequence of the GDPR's more rigorous accountability requirements means that organisations that handle personal data will need to operate a structured data protection compliance programme. The nature and extent of that programme will be specific to the organisation, dependent on its activities and the data it controls. However, in general terms data controllers will have to:

- Establish a data protection compliance program and privacy governance structure.
- Implement and maintain privacy controls on an ongoing basis (see Data Protection by Design and by Default).
- Embed ongoing privacy measures into internal policies and day-to-day activities, throughout the organisation.
- Leverage technology to require or ensure compliance (see Using Technical and Organizational Measures to Demonstrate Compliance).
- Maintain documentation of the privacy measures implemented and records of compliance.
- Train employees on privacy and data protection matters.
- Regularly test the privacy measures implemented.
- Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.

7.2 Do you need a data protection officer?

The appointment of a formal data protection officer is only required if data processing is carried out by a public authority or body, or the data controller and/or data processor's core activities involve either (i) the regular and systematic monitoring of data subjects on a large scale, or (ii) large-scale processing of sensitive personal data and personal data relating to criminal convictions and offenses.

7.3 Data protection by design and by default

These are concepts that have received much attention as far as the new GDPR is concerned. The principle of 'privacy by design' is that the GDPR requires data controllers to integrate data protection into their systems and product designs to ensure the inclusion of appropriate technical and organisational GDPR compliance measures into any data processing.

The concept of privacy by default requires the data controller to ensure that data is only processed for each specific business purpose.

The essence of both principles of privacy by design and default is to ensure that data protection is a part of an organisation's day to day activities at a cultural level, so that the concept of privacy is inherent in how the organisation behaves.

7.4 Organisational and technical measures

The practical application of some of these principles will vary from organisation to organisation. However, GDPR does recognise that the measures that an organisation may take will be appropriate to the level of risk involved. When assessing the appropriate level of security, the data controller or data processor should consider the risks presented by processing the personal data, including the risks associated with accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data. Risk assessments should therefore be undertaken.

Documenting the risk assessments made and the resulting decisions will go a long way to demonstrating compliance with GDPR.

Organisations that employ more than 250 people are subject to much more onerous recordkeeping requirements.

Contacts

London Office
2nd Floor, Rich Mix
35-47 Bethnal Green Road
London E1 6LA
T 020 7407 4625

Manchester Office
Green Fish Resource Centre
46–50 Oldham Street
Northern Quarter
Manchester M4 1LE
T 0161 234 2955

hello@theaudienceagency.org

www.theaudienceagency.org

Registered in England & Wales 8117915
Registered Charity No. 1149979