Additional Material for Chapter 28: Data Protection

The authors offer their sincere thanks to Olivia O'Kane, a specialist media and data protection lawyer in Belfast, and barrister Christopher Knight, of London chambers 11 KBW, for their help in the preparation of this material.

The new Data Protection Act 2018, which came into force on May 23, 2018, writes the EU's General Data Protection Regulation (GDPR) into the law of the UK. The intention of both the GDPR and the Act is to give individuals greater control of their data and introduce greater transparency and understanding about how personal data is collected and used.

Data controllers and processors – anyone who collects and/or uses information about people – may collect information that they need only for clear and specific purposes, and must ensure that it is kept safe. They must also ensure that data they keep is accurate, up-to-date, and relevant for a specified purpose allowed by law. News organisations – newspapers, magazine, websites and broadcasters – which keep information about people will qualify as data controllers and processors, as will freelance journalists who keep information about individuals, for example in contact books or on laptops or memory sticks.

Categories of data

Previous legislation categorised information as Personal Data and Sensitive Personal Data.
The GDPR and Data Protection Act 2018 replace these categories with 'personal data' and 'special category data'. Personal data is defined as 'any information relating to an identified or identifiable living individual'[1] – such as a name or 'one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity'.

Special category data is personal data which the GDPR regards as more sensitive, and so requires more protection. It includes personal data which reveals an individual's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership', as well as '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'[2]. Processing of special category data for purposes of journalism is subject to a higher test of 'substantial public interest' – rather than the 'public interest' test for personal data – and is permissible only where the journalism is related to 'unlawful acts and dishonesty etc'[3]. These are described as including the commission of an unlawful act, dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a body or association, and a failure in services provided by a body or association.

[1] DPA 2018 section 3(2)
[2] GDPR Article 9(1)
[3] DPA 2018 Schedule 1, Part 2, Paragraph 13

Data controllers and processors

News organisations and freelance journalists generally tend to be both data controllers and data processors – they are data processors when dealing with their internal data, and as data controllers when obtaining information from sources, other third parties, or customers and clients.

Data controllers control the purposes and means of processing personal data and must ensure that those with whom they work, such as third party data providers, also comply with the GDPR. A data processor processes personal data on the data controller's behalf. But remember, neither the controller nor the processor ever owns the personal data – it always belongs to the natural person – in the case of a journalist that might be the subject of the story or even the journalist's source, or in the case of the organisation it might be the data owned by a customer or the story subject.

Journalists working for news organisations and media groups should be able to rely on their organisations to ensure that their processes and policies comply with the requirements of the GDPR and the 2018 Act,. But all journalists should understand what those processes and policies are. Freelance journalists, and in certain circumstances employed journalists, need to understand what aspects of their activities fall under the titles of controller or processor, and then clearly define and document the activity they conduct and what consideration they gave to the privacy rights of the individuals whose data they hold.

The Act does not place an obligation on journalists generally to seek the consent of a data subject – an individual – referred to in a lawful public interest news report.

Exemptions

The exemptions in paragraph 26 of Part 5, Schedule 2 of the Data Protection Act 2018 mean that while personal data processed for the special purpose of journalism must be kept secure and protected from accidental damage or loss, it is exempt from various rights given under the GDPR where applying these would be 'incompatible with journalism' (one of the special purposes). These include the requirements[4] for:

- Lawful, fair and transparent processing;
- Collection for specified, explicit and legitimate purposes;
- Material to be adequate, relevant and limited to what is necessary;
- Material to be accurate and, where necessary, kept up to date;
- Material to permit identification of data subjects for no longer than is necessary.

The exemptions also protect material held for purposes of journalism from the rights of data subjects in relation to:

[4] Article 85(2) GDPR exempts for example: GDPR Article 5 (1) a-e (principles relating to processing); Article 6 (lawfulness); Article 7 (consent), Article 8(1), (2) (children's consent); Article 9 (special categories of data); Article 10 (criminal convictions); Article 14 (1)-(4) (data collected other than from data subject); Article 16 (rectification); Article 17(1), (2) (erasure) and so on.

- The identities of data controllers;
- The right of access to data held – the subject access request (see too, below: **Protection of Sources**;

- Erasure of the data;
- Rectification of errors;
- Restrict processing of the data.

But remember that these exemptions apply when the material is held for the purposes of journalism with a view to publication, and the data controller believes that publication would be in the public interest. The controller must, in deciding this issue, take account of 'the special importance of the public interest in the freedom of expression and information'[5]. In determining whether the publication would be in the public interest the data controller must have regard to the Ofcom Broadcasting Code, the Editors' Code or Practice or the BBC Editorial Guidelines (see chs. 2 and 3 of *McNae's* for context on these codes and the Guidelines).

It can be argued that journalists need, in the public interest, to be able to hold general background information about people who might figure in future news stories, not just those who already are the targets of investigations, or might become subjects of investigations.
But in any event, ne
ws organisations, journalists and freelance journalists should make sure that their processes and systems have proper security, such as full disk encryption on devices, locked cupboards, diligent checking of e-mails to make sure they ere not sent to the wrong person and so on. Any data breach, such accidental or unlawful destruction or loss, or unauthorised disclosure or access, must be reported immediately to the employer (and controller), who if required to report only has 72 hours within which to report the breach to the Information Commissioner's Office or Data Protection Office. Failure to report breaches within the 72-hour timeframe could lead to fines.

Exemptions are limited

Both the GDPR and the 2018 Act exemptions for the so-called 'special purposes' (e.g the purposes of journalism, and of academic, artistic or literary expression) are limited, and, like those in the 1998 Act, apply only to material which is being processed – *that is, kept and/or used* – for the purposes of journalism.

The news organisation or individual must be acting with the intention of publishing the material at some stage, must believe that publication is in the public interest, and have a reasonable belief that complying with the relevant provision in the Act is unsuited for journalism.

Any news organisation which is processing information for journalistic purposes must also be able to show at a later date that it has in place technical and organisational measures to ensure that all processing was and remains fair and lawful. This will involve being able to demonstrate, at some time in the future, that at the time the data was processed those responsible carefully considered

[5] Data protection Act 2018, Schedule 2, Part 5, Paragraph 26(4)

the public interest in processing it for the defined purpose of journalism against the impact on privacy rights, and that regard was also had to the relevant code – the Ofcom Broadcasting Code, the Editors' Code of Practice, or the BBC Editorial Guidelines – when the issue of the public interest of the publication or broadcast was being considered. These requirements are detailed in paragraph 26 of Part 5 of Schedule 2 to the 2018 Act.

A similar exemption applied for processing for journalistic purposes under section 32 of the Data Protection Act 1998.

Under the old legislation, it the Court of Appeal had held that the phrase 'view to publication' in the exemption granted under section 32 did not just apply to the period before publication (*Naomi Campbell v MGN Ltd.* [2002] EWCA Civ 1373; [2003] EMLR 2; [2003] HRLR 2; [2003] QB 633; [2003] 2 WLR 80; [2003] 1 All ER 224). Lord Phillips, Master of the Rolls, said that any finding to the contrary would 'would impose restrictions on the media which would radically restrict the freedom of the press'.

Thus, the exemption did not expire as a result of publication, and so the law did not require a media organisation ('as data controller') to order its journalists to delete - or release in response to a 'subject access request' - information gathered for journalistic purposes about a person just because some of it had been published.

It seems likely that the court will continue to follow that view now that the GDPR and the 2018 Act are in force. First, the wording of the exemption is virtually the same, and in addition Recital 152 of the GDPR requires that 'In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.'

An indication of the view the courts might take on the issue of whether material is actually being held for the purposes of journalism might be gained from the case of *Steven Sugar v The British Broadcasting Commission & Another* ([2010] EWCA Civ 715; [2010] EMLR 24; [2010] 1 WLR 2278). This was an attempt by a solicitor to use the Freedom of Information Act 2000 to obtain a copy of the Balen Report, an internal BBC report analysing its coverage of the Middle East and the Israeli-Palestinian conflict. The Information Tribunal – now the First Tier Tribunal – had ordered the BBC to release the document on the grounds that as it was not only being held for the purposes of journalism it was not protected from disclosure by the relevant exemption in the Freedom of Information Act. But the Court of Appeal, headed by the Master of the Rolls, Lord Neuberger, upheld a High Court ruling overturning that decision, ruling that it could well have a chilling effect on BBC journalism if any document held for journalistic purposes and another purpose was liable to be disclosed to the public.

Lord Neuberger said:

> 'However, although "the public's right to know", in the sense of having access to information held by government and other public bodies, is a very important aspect of a modern, free

> and democratic society, it is a general right, which, as it seems to me, can be expected to yield to society's more specific public interest in the media being free from the sort of constraints which would arise if journalism-related thoughts, investigations, or discussions could not be freely conducted within organisations such as the BBC. Sunlight is the best disinfectant, but it can also burn, and when it comes to information held by the BBC for the purposes of journalism, it seems to me that the legislative policy is that the risk of burning outweighs the benefit of disinfectant.'

Sensitive personal data under the old legislation

The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417) is a statutory instrument which sets out 10 circumstances in which 'sensitive personal data' may be lawfully processed.

This statutory instrument remains in force in relation to claims brought under the Data Protection Act 1998 and the regime pre-dating the coming into force in May 2018 of the GDPR and the 2018 Act. Neither the Statutory Instrument nor the 1998 Act apply after May 2018.

But much of what is in the Statutory Instrument has been amalgamated into the 2018 Act.
Several of the circumstances under which 'sensitive personal data' was publishable require that the processing must be 'in the substantial public interest'. For journalists the most important was in paragraph 3, which covers disclosures for journalistic, artistic, or literary purposes of personal data relating to:

- the commission by any person of any unlawful act (whether alleged or established);
- dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established); or
- mismanagement in the administration of, or failures in services provided by, any body or association (whether alleged or established).

These and other parts of this instrument provide what are in effect 'public interest' defences as regards the processing of data.

Why did this statutory instrument not provide a defence to the *Daily Mirror* in the case – outlined in 27.1 and 28.5.2 of *McNae's* – concerning Naomi Campbell? Remember that processing of data must also be 'fair and lawful'. As the House of Lords reached the decision that the *Daily Mirror* coverage of Naomi Campbell's therapy for drug abuse was a breach of confidence, it could not be said to be 'lawful' processing.

Protection of sources

People have the right under the Data Protection Act 2018 to discover whether a 'data controller' holds information about them, and, if so, what it is. This is known as a 'subject access request'. They must also be told the purposes for which it is held - for example, journalism - to whom it is or may be disclosed; and the origin of the information.

A person may send a subject access request to a media 'data controller' to attempt to find out, by asking for information about himself/herself, or asking about other information the news organisation or journalist holds. In some circumstances the very nature of such information, to a requester who gets hold of it, might make the identity of the source obvious, so for the journalist to reveal any of it would betray that source. But a ' data controller' has the right not to comply with an access request if the material is held for 'journalistic, literary, or artistic purposes' and so is covered by the exemption in paragraph 26 of Part 5 of Schedule 2 to the 2018 Act.

> **Case study**: The *Mid Devon Gazette* published a story about how Cullompton Town Council had held finance meetings in private, against regulations. It was written after a copy of a council email was leaked to the paper. The council and a former town councillor, Ashley Wilce, who had been denied access to a meeting, asked the paper for a copy of the email, but the Gazette refused, saying this could have led to its source being identified. Mr Wilce complained to the Information Commissioner's Office, saying that the Gazette was breaching the Data Protection Act 2018 in its refusal. The paper, to justify its position, told the ICO that under section 32 of the Act it had an exemption in respect of data held for journalistic purposes and used in the public interest. The ICO case officer later told the paper the investigation into the complaint had closed, because 'it is likely that the Mid Devon Gazette has complied with the requirements of the Act' (*Holdthefrontpage*, 19 July 2012).

Given the other protections which are also available for protecting journalists' sources, including the right to freedom of expression under Article 10 of the European Convention on Human Rights, the best advice for journalists is that they do not have to name a source or disclose information about a source likely to lead to their identity unless there is a court order compelling them to disclose any information pertaining to that source – in which case, of course, they have to consider whether to refuse to do so anyway because of their ethical and moral obligations, as 34.1 and 34.2 in *McNae's* explains.

Powers of entry and inspection

The 2018 Act gives the Information Commissioner wide powers of entry and inspection in relation to data held by data controllers. These powers can be exercised only under a warrant granted by a circuit judge (in Northern Ireland by a county court judge). A judge must not issue a warrant relating to personal data processed for the 'special purposes' (including journalism) unless the Commissioner has decided whether such data fall within the special purposes exemption.

As yet, there has been no example of the Commissioner 'raiding' the premises of media organisations for material being held ('processed') for journalism.

Guidance for the media on data law

Sir Brian Leveson, in his report into 'the culture, practices, and ethics of the press' (see 2.1.1 in *McNae's*) recommended that the Information Commissioner should issue 'comprehensive good

practice guidelines and advice on appropriate principles and standards to be observed by the press in the processing of personal data'.

Sir Brian had pointed out that: 'The Operation Motorman "treasure trove" constituted evidence of serious and systemic illegality and poor practice in the acquisition and use of personal information which could have spread across the press as a whole.' Operation Motorman was the inquiry - referred to in 28.3 in *McNae's* - which led to the conviction of private investigator Steve Whittamore for breach of the Data Protection Act 1998. Whittamore's clients included several national newspapers. No newspapers were ever prosecuted as a result of the inquiry.

In September 2014 the Commissioner, responding to Leveson's report, issued the document 'Data Protection and Journalism; a guide for the media'. At the time this piece was being written, in August 2018, that guide – which was said to be intended to 'help journalists, editors, and managers understand and comply with data protection law and good practice, while recognising the vital importance of a free and independent media' – was in the process of being re-written to reflect the changes introduced by the GDPR and Data Protection Act 2018. The updated guidance has not yet been published.

The old guidance did give reassurance that a media organisation or journalist faced with a 'subject access request' could remove from the requested material the identity of confidential sources 'as long as it is reasonable to do so'.