cornerstone barristers

Civil penalties under the data protection regime

Philip Coppel QC

Thursday, 19 May 2022

Timeline of data protection: early days

- 23 September 1980 – OECD recommended guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- 28 January 1981 – Council of Europe Convention for the protection of individuals with regard to the Automatic Processing of Personal Data (“Convention 108”)
- 12 July 1984 – Data Protection Act 1984

Timeline of data protection: 1998-2018

- 24 October 1995 - Directive 95/46/EC
- 2 October 1997 – Treaty of Amsterdam signed
- 16 July 1998 – Data Protection Act 1998 comes into force
- 9 November 1998 – Human Rights Act 1998 comes into force
- 2000 – Charter of Fundamental Rights proclaimed
- 1 December 2009 – Treaty of Lisbon comes into force, making the Charter enforceable

Penalties and the DPA 1998

- Sections 55A-55E introduced in 2008 by section 114 of the Criminal Justice and Immigration Act 2008:

"**55A Power of Commissioner to impose monetary penalty**

(1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—

(a) there has been a serious contravention of section 4(4) by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller—

(a) knew or ought to have known—

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention…."

Penalties under DPA 98 in practice

Leveson and penalty practice…

Recommendations to the Information Commissioner

58. The Information Commissioner's Office should take immediate steps to prepare, adopt and publish a policy on the exercise of its formal regulatory functions in order to ensure that the press complies with the legal requirements of the data protection regime.[59]

59. In discharge of its functions and duties to promote good practice in areas of public concern, the Information Commissioner's Office should take immediate steps, in consultation with the industry, to prepare and issue comprehensive good practice guidelines and advice on appropriate principles and standards to be observed by the press in the processing of personal data. This should be prepared and implemented within six months from the date of this Report.[60]

Common law and personal privacy

House of Lords

Wainwright *v* Home Office

[2003] UKHL 53

2003 July 1, 2, 3;
Oct 16

Lord Bingham of Cornhill, Lord Hoffmann,
Lord Hope of Craighead, Lord Hutton
and Lord Scott of Foscote

Tort — Cause of action — Intentional infliction of harm — Visitors to prison strip-searched for drugs — Distress and humiliation inflicted — Whether infringement of right to respect for private life — Whether cause of action

The claimants, a mother and son, were strip-searched for drugs on a prison visit in 1997. The search was not conducted according to rule 86 of the Prison Rules 1964, and the claimants were humiliated and distressed. No drugs were found. The second claimant, aged 21, who was mentally impaired and suffered from cerebral palsy, developed post-traumatic stress syndrome. They claimed damages for trespass, and the second claimant claimed, in addition, damages for battery. The judge held that trespass to the person, consisting of wilfully causing a person to do something to himself which infringed his right to privacy, had been committed against both claimants, and, further, that trespass to the person, consisting of wilfully causing a person to do something calculated to cause harm to him, namely infringing his legal right to personal safety, had been committed against the second claimant, as had battery. He awarded basic and aggravated damages of £2,600 to the first claimant and £4,500 to the second claimant. The Court of Appeal allowed the Home Office's appeal against the finding of trespass, dismissed the first claimant's claim and reduced the award of damages to the second claimant.

On appeal by the claimants—

Held, dismissing the appeals, (1) that there was no common law tort of invasion of privacy; that the creation of such a tort required a detailed approach which could be achieved only by legislation rather than the broad brush of common law principle; that adoption of a right to privacy as a principle of law in itself was not necessary to comply with article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; and that any gaps in existing remedies for breaches of article 8 by public authorities had been filled by sections 6 and 7 of the Human Rights Act 1998 (post, paras 1, 30–35, 52–56, 64).

The common law again: Campbell v Mirror Newspapers, HL 2004

Confidential information

255 As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ("confidential") information. It is important to keep these two distinct. In some instances information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. Privacy can be invaded by further publication of information or photographs already disclosed to the public. Conversely, and obviously, a trade secret may be protected as confidential information even though no question of personal privacy is involved. This distinction was recognised by the Law Commission in its report on Breach of Confidence (1981) (Cmnd 8388), pp 5–6.

Charter of Fundamental Rights

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 16 TFEU

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Regime change - 2018

- 14 April 2016 – Council of Europe and European Parliament adopt “the data protection package”, ie the Law Enforcement Directive + GDPR, requiring implementation by 25 May 2018.
- 25 May 2018 – GDPR takes effect.
- 25 May 2018 – LED takes effect.
- 25 May 2018 – Data Protection Act 2018 takes effect.
- 10 October 2018 – UK signs the protocol “modernising” Convention 108.

The new architecture

Data Protection Act 2018

CHAPTER 12

CONTENTS

GDPR & DPA: the inter-relationship

PART 1

PRELIMINARY

1 Overview

(1) This Act makes provision about the processing of personal data.

(2) Most processing of personal data is subject to the GDPR.

(3) Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter 3).

(4) Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.

(5) Part 4 makes provision about the processing of personal data by the intelligence services.

(6) Part 5 makes provision about the Information Commissioner.

(7) Part 6 makes provision about the enforcement of the data protection legislation.

GDPR and penalties: the basics

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

GDPR and penalties: the criteria

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

GDPR and penalties: the amount

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 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:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

DPA 2018 and penalties: the start

Enforcement notices

149 Enforcement notices

(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice,

or both (and see also sections 150 and 151).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

DPA 2018: the penalty notice

Penalties

155 Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2), (3), (4) or (5), or

(b) has failed to comply with an information notice, an assessment notice or an enforcement notice,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

DPA 2018: the criteria

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) Those matters are—

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 57, 66, 103 or 107;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) whether the penalty would be effective, proportionate and dissuasive.

DPA 2018: the amount

157 Maximum amount of penalty

(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) the amount specified in Article 83 of the GDPR, or

(b) if an amount is not specified there, the standard maximum amount.

Penalties: Commissioner Guidance

Guidance

160 Guidance about regulatory action

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's functions in connection with—

(a) information notices,

(b) assessment notices,

(c) enforcement notices, and

(d) penalty notices.

(2) The Commissioner may produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's other functions under this Part.

(7) In relation to penalty notices, the guidance must include—

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties;

(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.

Information Commissioner guidance

Penalty notices: the ICO criteria

When a Penalty Notice will be appropriate

In the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations. These will typically involve wilful, deliberate or negligent acts, or repeated breaches of information rights obligations, causing harm or damage to individuals. In considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction.

This means that each case will be assessed objectively on its own merits. But our hierarchy and risk-based approach mean that it is more likely that a penalty will be imposed where, for example:

- a number of individuals have been affected;
- there has been a degree of damage or harm (which may include distress and/or embarrassment);
- sensitive personal data has been involved;
- there has been a failure to comply with an information notice, an assessment notice or an enforcement notice
- there has been a repeated breach of obligations or a failure to rectify a previously identified problem or follow previous recommendations.;
- wilful action (including inaction) is a feature of the case;
- there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it); and
- there has been a failure to implement the accountability provisions of the GDPR.

The hierarchy

A hierarchy of regulatory action

We will consider each case on its merits and within the context of any compliance breach (or risk of such breach). However, as a general principle, the more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action. Breaches involving novel or invasive technology, or a high degree of intrusion into the privacy of individuals, without having done a full Data Protection Impact Assessment and taken appropriate mitigating action and/or which should have been reported to the ICO[21] but was not, can also expect to attract regulatory attention at the upper end of the scale.

Our regulatory approach generally represents a range of measures. This spans observation, intelligence gathering and monitoring through to individual case and appeal considerations, as well as application of audit/assessment or inspection powers to better understand an issue, and, then, finally investigation and sanction where we need to look at and address the detail of an incident.

In this way, as issues or patterns of issues escalate in frequency or severity then we will use more significant powers in response. This does not mean however that we cannot use our most significant powers immediately in serious or high-risk cases where there is a direct need to protect the public from harm.

Our approach will also encourage and reward compliance. Those who self-report, who engage with us to resolve issues and who can demonstrate strong information rights accountability arrangements, can expect us to take these into account when deciding how to respond.

We will also provide opportunities for innovative products, services or concepts to be tested with appropriate regulatory oversight and safeguards, so that innovation and development is not over-burdened.

Penalty notices: asking others

Where appropriate, we will also have regard to representations (including from any Concerned Supervisory Authorities elsewhere in the EU where the ICO is the lead Supervisory Authority or the Data Protection Board itself) under the cooperation and consistency mechanisms of the GDPR in setting the final amount of any penalty. These representations will be taken after the consideration of representations of the target of the penalty but before the final setting of any penalty level and following the procedures set out in relevant Data Protection Board rules of procedure.

Penalty notices: representations

Representations will be taken from the proposed target about the imposition of the penalty and its level. The target will be allowed at least 21 calendar days to make these representations.

In addition, we may allow an organisation or individual subject to an NOI to submit representations orally during a face-face meeting at our office. However, this is discretionary and only relevant in cases that are considered by us to be exceptional. It is likely that these could be appropriate in circumstances where:

- the central facts of any breach or failing are in dispute;
- the integrity of any technical witness evidence is in dispute;
- there is a requirement to make reasonable adjustments under the Equality Act 2010; or
- the consideration of 'harm' elements of a case would benefit from evidence from those affected.

The 5 step approach

What will be the amount of any penalty

Where we have discretion to set the amount of any penalty in the context of our regulatory work, we will approach setting any penalty level, within the legislative bands, on the basis of the following mechanism:

Step 1. An 'initial element' removing any financial gain from the breach.

Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) of the DPA.

Step 3. Adding in an element to reflect any aggravating factors.

Step 4. Adding in an amount for deterrent effect to others.

Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).

The appeal right

162 Rights of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal—

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(3) A person who is given a penalty notice or a penalty variation notice may appeal to the Tribunal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

The nature of the appeal

163 Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 162(1) or (3).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers—

(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

Deference?

Court of Appeal

Regina (Hope and Glory Public House Ltd) *v* City of Westminster Magistrates' Court

[2011] EWCA Civ 31

2010 Nov 9;
2011 Jan 26

Sir Nicholas Wall P, Laws, Toulson LJJ

Licensing — Licensed premises — Appeal to magistrates' court — Licensing authority's decision on review of licence — Whether appeal only to be allowed if magistrates' court satisfied original decision wrong — Whether onus on appellant to prove case on appeal breaching right to fair trial — Whether appeal process Convention compliant — Whether magistrates' court having power to correct error of law by licensing authority — Human Rights Act 1998 (c 42), Sch 1, Pt I, art 6.1[1] — Licensing Act 2003 (c 17), s 181, Sch 5, para 8[2] — Magistrates' Courts Rules 1981 (SI 1981/552), rr 14, 34[3]

41 As Mr Matthias rightly submitted, the licensing function of a licensing authority is an administrative function. By contrast, the function of the district judge is a judicial function. The licensing authority has a duty, in accordance with the rule of law, to behave fairly in the decision-making procedure, but the decision itself is not a judicial or quasi-judicial act. It is the exercise of a power delegated by the people as a whole to decide what the public interest requires: see the speech of Lord Hoffmann in the *Alconbury* case [2003] 2 AC 295, para 74.

48 It is normal for an appellant to have the responsibility of persuading the court that it should reverse the order under appeal, and the Magistrates' Courts Rules 1981 envisage that this is so in the case of statutory appeals to magistrates' courts from decisions of local authorities. We see no indication that Parliament intended to create an exception in the case of appeals under the Licensing Act 2003.

cornerstone barristers

The end

Philip Coppel QC

Thursday, 19 May 2022