CONTENTS

Part I Overview

Part V Exemptions

CHAPTER 7

Data protection: introduction

1. ORIGINS OF DATA PROTECTION LAW

7– 001 Meaning of data protection

The essence of data protection is the legislative control over the extent to which and the manner in which information about an individual may be used by others, and the correlative extent and manner that those others are permitted to use information about an individual. The word 'use' here covers the complete life-cycle of information: acquisition, storage, organisation, retrieval, consultation, reliance, adaptation, copying, dissemination, publication, blocking, erasure and destruction. The legislative control seeks to accommodate and, so far as possible, reconcile the two interests that are within the concept of data protection: (a) the interest of an individual that information relating to him or herself should not be misused or over-used; and (b) the interest of a user of that personal information in being permitted due use of it. The need for and nature of data protection reflect information not in itself being a species of property,

with the consequence that the panoply of rights and correlative obligations attaching to property and enforceable at law are inapplicable to personal information.[1] For this reason, it is an unhelpful distraction to look to property law for answers to issues in data protection law.

7– 002 Approach of data protection law

Data protection law aims to protect the rights of identifiable living individuals ('data subjects') as regards anything done ('processing') with information relating to them ('personal data') by or on behalf of persons who determine how and for what purposes that information is used ('controllers'). It does so by imposing a range of continuing obligations on controllers and those acting on their behalf ('processors') in respect of all processing of personal data ('principles'), as well as by conferring specific rights that data subjects can assert against a data controller. Although these rights will often overlap with the ordinary conception of a right to personal privacy, there is no requirement that personal privacy be infringed in order for data protection obligations or rights to be infringed: the obligations and rights are inherent in the processing of personal data. Thus, data protection law recognises that where, for example, a controller has, without the consent of a data subject, abstracted his or her personal data, that data subject will have an actionable claim against the controller without needing to support that claim with an allegation of resultant pecuniary loss or resultant distress.[2] The rights and obligations are legislatively shaped in order not to impede recognised interests making legitimate use of that information.

7– 003 In the beginning

Until well into the 1990s, courts in the United Kingdom, while occasionally acknowledging shortcomings in the common law's protection of personal privacy,[3] invariably declined to protect a person from aspects of his or her personal life being watched, recorded or disseminated to others unless there was something more to it — eg a confidential relationship.[4]

---

1 That data is not per se regarded as a species of property has been repeatedly recognised: *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1 at [275]-[276]; *Phillips v News Group Newspapers Ltd* [2012] UKSC 28, [2013] 1 AC 1 at [30]; *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281, [2015] QB 41; *Environment Agency v Churngold Recycling Ltd* [2014] EWCA Civ 909, [2015] Env LR 13 at [16]-[19]; *Computer Associates UK Ltd v Software Incubator Ltd* [2018] EWCA Civ 518, [2018] 2 All ER (Comm) 398; *Various Claimants v Morrison Supermarkets plc* [2018] EWCA Civ 2339, [2019] QB 772 at [44]-[45]; *Lloyd v Google LLC* [2019] EWCA Civ 1599, [2020] EMLR 2 at [46]; *Ramsden v HMRC* [2019] EWHC 3566 (QB) at [99]. See also the authorities cited at §20– 038.

2 See *Lloyd v Google LLC* [2019] EWCA Civ 1599, [2020] EMLR 2 at [45]-[70]. Although in that case the wrong suffered was labelled a 'loss of control' of the personal data, whether a data subject ever had, or wished to exert, that control should make no difference to the existence of the wrong: the true wrong lies in the misuse and over-use of the data subject's personal data, regardless of resultant pecuniary loss, regardless of resultant distress and regardless of whether the data subject ever had or exerted control. In this respect it is like trespass to goods or land, neither of which require loss and both of which take account of the extent of the interference and the benefit had by the defendant in assessing the damages to be awarded. Other authorities have recognised that mere interference with personal data is sufficient to provide the data subject with a basis for claim: *Re EU-Canada Passenger Name Record (PNR) Agreement* [2018] 1 CMLR 1083 at [124] ('it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference'); *Schrems v Data Protection Commissioner* (C-362/14) [2016] QB 527, [2016] 2 CMLR 2 at [87]; *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12 and C-594/12) [2015] QB 127, [2014] 3 CMLR 44 at [33].

3 For example: *Turner v Spooner* (1861) 30 LJ Ch 801 at 803; *Monson v Tussauds Ltd* [1894] 1 QB 671 at 687; *Tolley v Fry Ltd* [1930] 1 KB 467 at 478 per Greer LJ; reversed on appeal [1931] AC 333; *Victoria Park Racing v Taylor* (1937) 58 CLR 479 at 505, per Rich J (diss); *Bernstein v Sky Views* [1978] QB 479 at 483; *Kaye v Robertson* [1991] FSR 62 at 70 (CA); *R v Khan (Sultan)* [1997] AC 558 at 582-583; *Mills v News Group Newspapers Ltd* [2001] EWHC Ch 412 ('But the day may not be far off when this deficiency will be remedied'); *A v B plc* [2002] EWCA Civ 337, [2003] QB 195; *Douglas v Hello! Ltd* [2003] EWHC 786, [2003] 3 All ER 996 at [229]; cf *Morris v Beardmore* [1981] AC 446 at 465.

4 In *Prince Albert v Strange* (1849) 1 Mac & G 25, 41 ER 1171, (1849) 1 De G & Sm 652 Knight-Bruce VC referred to a 'sordid spying into the privacy of domestic life' (DeG & Sm at 698) and, on appeal, Lord Cottenham LC spoke of privacy as the right being invaded (1 Mac & G at 47). However, the Court did treat the case as one of an interference with the plaintiff's property, namely his right to publish the etchings (DeG & Sm at 697). While it is

This contrasted with the position in the USA. An article by Warren and Brandeis published in 1890[5] had proved seminal in the development of a legal right of privacy. By 1960 the common law in that country had sufficiently developed to recognise that 'privacy' was not a unitary concept:

> The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by a common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff....to be let alone.[6]

Such concepts remained alien in the United Kingdom: without any external impetus, there was no need to pretend that the common law was vibrant or adapted to the needs of the age. In February 1961 Lord Mancroft introduced a Right of Privacy Bill into the House of Lords.[7] The stated object of the Bill was:

> to give every individual such further protection against invasion of his privacy as may be desirable for the maintenance of human dignity while protecting the right of the public to be kept informed in all matters in which the public may be reasonably concerned.[8]

The method used to achieve this was to confer on a person a right of action:

> against any other person who without his consent publishes of or concerning him in any newspaper or by means of cinematograph exhibition or any television or sound broadcast any words relating to his personal affairs or conduct if such publication is calculated to cause him distress or embarrassment.

The Bill then provided for various defences. The Bill did not survive the Parliamentary Session. In an article in1962, Brian Neill pressed for legal protection for privacy, observing that it was expressly provided for in Art 12 of the Universal Declaration of Human Rights and Article 8(1) of the European Convention on Human Rights.[9] Between 1967 and 1980 the lack of legal protection for privacy had been the target of five parliamentary bills,[10] two parliamentary reports,[11] two White Papers[12] and a Law Commission working paper. The sentiments expressed within them remained just that.

7– 004 International instruments

At the international level, the right to a private domain had been recognised in Art 12 of the Universal Declaration of Human Rights, adopted and proclaimed by the United Nations on 10 December 1948. Although a non-binding declaration, the Universal Declaration has always

possible that the identity of the parties informed the outcome, for the next 150 years equity and the common law rested.

5 'The Right to Privacy', *Harvard Law Review*, vol 4, 1890, 193.

6 Prosser, 'Privacy' *California Law Review*, vol 48, 1960, 383 at 389. Professor Prosser taxonimised 'privacy' into four classes: (1) an intrusion upon the plaintiff's physical solitude or seclusion (including unlawful searches, telephone tapping, long-distance photography and telephone harassment); (2) a public disclosure of private facts; (3) publicity putting the plaintiff in a false light; and (4) an appropriation, for the defendant's advantage, of the plaintiff's name or likeness. The taxonomy does not provide an ideal fit with English jurisprudence. It is partly shaped by the premium placed on free speech under the US Constitution. 'Data protection' is principally concerned with (1) and (2), with (3) being protected through the law of defamation and (4) being protected through various intellectual property rights. Class (1) may also give rise to a claim in private nuisance: see *Fearn v Tate Gallery* [2019] EWHC 246 (Ch), [2019] Ch 369 at [133]-[179].

7 *Hansard* HL vol 229, col 660.

8 Explanatory memorandum.

9 'The Protection of Privacy', *Modern Law Review*, vol 25, 1962, 393. The author subsequently became Neill LJ.

10 Introduced by: Mr Lyon, 1967; Mr Walden, 1968; Mr Kenneth Baker, 1969; Mr Huckfield, 1971; Lord Manocroft, 1971.

11 *Report on the Committee on Privacy* – called 'the Younger Report' – (Cmnd 5012, 1972), which established 10 principles for the handling of personal data, and the *Report on the Committee on Data Protection* – called 'the Lindop Committee Report' – (Cmnd 7341, 1978).

12 *Computers and Privacy*, Cmnd 6353, 1975; and *Computers: Safeguards for Privacy*, Cmnd 6354, 1975.

had considerable status as the foundational instrument of international human rights law. On 16 December 1966 the General Assembly of the United Nations resolved to adopt the International Covenant on Civil and Political Rights, Art 17 of which reproduced Art 12 of the Universal Declaration:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The United Kingdom signed the Covenant on 16 September 1968 and ratified it on 20 May 1976.

7– 005 Council of Europe

The Council of Europe was founded on 5 May 1949 by the Treaty of London.[13] It has the stated aim of upholding human rights, democracy and the rule of law in Europe. It currently has 47 Member States, of which 28 are Member States of the EU. It does not make binding laws, but it does enforce select international agreements to which its Member States are parties. The ECHR is an instance of such an international agreement, and the ECtHR is a body of the Council which enforces the ECHR. The Council's three statutory bodies are the Committee of Ministers (comprising the foreign ministers of each Member State), the Parliamentary Assembly (composed of members of the national parliaments of each Member State and which adopts resolutions and makes recommendations to all Member States). and the Congress of Local and Regional Authorities (currently comprising 648 members holding elective regional, mayoral or municipal office in the different Member States). In 1968, the Parliamentary Assembly addressed Recommendation 509 to its Committee of Ministers, asking it to examine whether the ECHR and the domestic law of the Member States offered adequate protection to the right of personal privacy vis-à-vis modern science and technology. A study carried out on instruction of the Committee of Ministers in response to that Recommendation showed that national legislation gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks. It was the first recognition that regulation of the use of personal information need not always be coincident with the protection of personal privacy and of an individual's elemental right to limit other's use of personal information about him or herself. On the basis of these findings, the Committee of Ministers adopted in 1973 and 1974 two resolutions on data protection. The first – Resolution (73) 22 – established principles of data protection for the private sector. The second – Resolution (74) 29 – did the same for the public sector. Within five years after the passing of the second resolution, general data protection laws had been enacted in seven Member States (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway and Sweden).[14] For its part, the United Kingdom turned its face against such regulation. In 1974, its status as a so-called 'data haven' (ie a country with no legal control over or regulation of the use of personal data) resulted in the Swedish Data Inspector Board banning the export of Swedish personal data to the United Kingdom under the terms of that country's Data Act 1973. This forced the United Kingdom to re-visit its position, in the first instance by commissioning what became the Lindop Committee. It proved to be a slow business, with an institutional reluctance to participate, let alone assist.[15] Meanwhile, in three Member States, data protection had been

[13] The original signatories were Belgium, Denmark, France, Ireland, Italy, Luxembourg, Netherlands, Norway, Sweden and the United Kingdom. The idea of such a body had been urged by Sir Winston Churchill in an address to the University of Zurich on 19 September 1946.

[14] In 1970 the German state of Hesse adopted the world's first data protection law: Hessisches Datenschutzgesetz. It applied only to that state. in 1973 Sweden adopted the Datalagen. In 1976 Germany adopted the Bundesdatenschutzgestez. And in 1977 France adopted the Loi relatif à l'informatique, aux fichiers et aux libertés.

[15] For a fuller account, see: Warren and Dearnley 'Data Protection Legislation in the United Kingdom from development to statute 1969-84', *Information, Communication & Society*, vol 8, no 2, June 2005, pp 238-263.

incorporated as a fundamental right in the Constitution (Article 35 of the 1976 Constitution of Portugal; Article 18 of the 1978 Constitution of Spain; Article 1 of the 1978 Austrian Data Protection Act: Fundamental Right of Data Protection).

7– 006 OECD

Developments in data protection were not confined to Europe. On 23 September 1980 the Council of the Organisation for Economic Co-operation and Development – the OECD – adopted a 'Recommendation concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.'[16] The paramount concern of the recommended guidelines was to prevent adverse economic consequences of different national standards governing the processing of personal information, which the OECD characterised as a barrier to trade and which it recognised was acutely significant for the rapidly growing processing of data by computers.[17] The OECD guidelines accommodated the competition of interests between the member countries advocating the greatest freedom in transborder data flows (principally the USA) and those member countries placing greater emphasis on the protection of individual rights (principally certain European countries). The Guidelines defined terms that were to become familiar in the field – 'data controller'[18] and 'personal data'[19] – and set out eight 'basic principles of national application'[20] and four 'basic principles of international application.'[21] On 11 July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data – 'The OECD Privacy Guidelines' – the first revision since the 1980 guidelines.

7– 007 Council Convention 108

On 28 January 1981 the Council of Europe opened the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data – 'Convention 108.' The Convention applies to all data processing carried out, whether in the private sector or in the public sector, including data processing by the judiciary and law enforcement agencies. The Convention remains in force. Article 1 states that its purpose is to secure for every individual:

> respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').

---

16 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted 23 September 1980. The background to the OECD involvement is summarised in an article by the Chairman of the expert group that was tasked with preparing its guidelines: Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy', *International Data Privacy Law*, 2011, vol 1, no 1, 6-14.

17 'One normally thinks of the OECD as a body of sober economists, statisticians, and technologists. One does not normally expect such people to be dripping with human rights sentiments.': Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy', *International Data Privacy Law*, 2011, vol 1, no 1, at p 6.

18 The Guidelines defined 'data controller' for the purposes of the Guidelines to mean 'a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.'

19 The Guidelines defined 'personal data' for the purposes of the Guidelines to mean 'any information relating to an identified or identifiable individual.'

20 These were: (1) a collection limitation principle; (2) a data quality principle; (3) a purpose specification principle; (4) a use limitation principle; (5) a security safeguards principle; (6) an openness principle; (7) an individual participation principle; and (8) an accountability principle.

21 These were: (1) each Member country taking into consideration the implications for other Member countries of domestic processing and re-export of personal data; (2) each Member country taking reasonable and appropriate steps to ensure that transborder flows of personal data were uninterrupted and secure; (3) each Member country refraining from restricting transborder flows of personal data between itself and another Member country, with certain limitations; and (4) each Member country avoiding developing laws, policies and practices in the name of protecting privacy that created obstacles to the transborder flow of personal data that would exceed the requirements for such protection.

Although its stated purpose places the use of personal information within the concept of the right to privacy, the scope of the Convention (Art 3) is unrelated to privacy and the statement of basic principles (Arts 4 to 11) is similarly unrelated.[22] This was an even clearer recognition of an individual's elemental right to limits on the use made of private information relating to him or herself than the Council of Europe's Recommendation 509.

7– 008 Convention 108 content

The Convention provides definitions of 'personal data,'[23] 'data subject' and 'controller of the [automated data file].' Article 5 provides the central set of principles governing the processing of personal data:

> Personal data undergoing automatic processing shall be:
> (a) obtained and processed fairly and lawfully;
> (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
> (d) accurate and, where necessary, kept up to date;
> (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The Convention recognises that certain categories of personal data are particularly sensitive, requiring special safeguards for their processing.[24] The Convention provides that a data subject should be able to request information to establish the existence of 'an automated personal data file' and to secure a copy of it and, where it has not been processed in accordance with the principles, to rectify or erase it.[25] Various exceptions on the usual basis – protecting State security, public safety and the rights and freedoms of others etc – are provided for.[26] Reflecting the OECD's other concern, the Convention also provides that transborder flows of personal data are not to be prohibited or subject to special authorisation for the sole purpose of protecting privacy.[27] The United Kingdom signed the Convention on 14 May 1981 and ratified it on 26 August 1987. As at January 2020, 55 parties have signed and ratified the Convention, including Mexico, Uruguay, all EU countries, Switzerland, Russia, Turkey and other Member States of the Council of Europe. Amendments made to the Convention in 2018 have not yet been ratified or come into force.[28]

7– 009 DPA 1984

By signing Convention 108, the United Kingdom had signified its willingness to enact data protection legislation. In April 1982 a White Paper[29] was published. It said that legislation was needed because of the threat to privacy posed by the rapid growth in the use of computers. But, in a nod to the earlier troubles with Sweden,[30] it also recognised that when the Convention came into force those countries with data protection legislation in place would be able to refuse

---

22 The reference to privacy in Art 9(3) is confined to use of personal data for statistics or scientific research purposes.

23 Identical to the OECD's definition.

24 Article 6.

25 Article 8.

26 Article 9.

27 Article 12.

28 Effected by Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS no 223.

29 *Data Protection: the Government's Proposals for Legislation* (Cmnd 8539).

30 See §7– 005 above.

to allow personal data to be sent to countries that did not have such legislation in place. In December 1982 a data protection bill was introduced in the House of Lords but, after passing in the House of Commons, it failed to achieve enactment before Parliament was dissolved in 1983. A new bill was introduced in the House of Lords and, after being passed by both Houses, on 12 July 1984 it received Royal Assent. The Data Protection Act 1984 drew on the principles fashioned by the OECD Recommendation and the Council of Europe's Convention, as well as the Younger Report and Lindop Committee Report. The DPA 1984 did not once use the word 'privacy.' Although the DPA 1984 did not adopt all the reports' recommendations on the protection of privacy, it did provide a measure of protection against the mishandling of personal, private information. The individual was given limited rights to bring a claim against a data controller, with most non-compliance to be dealt with by the data protection registrar.[31] That the Act's dual object was to protect against the misuse and over-use of personal information as well as to ensure the free movement of data was recognised in the only authority on the DPA 1984 to reach the House of Lords:[32]

> My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.
>
> English common law does not know a general right of privacy and Parliament has been reluctant to enact one. But there has been some legislation to deal with particular aspects of the problem. The Data Protection Act 1984, with which this appeal is concerned, is one such statute....The Act was therefore intended not only to protect the privacy of our own citizens but to provide sufficient safeguards for the protection of computerised personal information to satisfy other member states that such information could safely be exported to the United Kingdom.

Such insight was the exception, with ignorance, impatience and hostility being the norm. In 1990 a further report on privacy was laid before Parliament.[33]

2. DIRECTIVE 95/46/EC & DPA 1998 REGIME

7– 010 The Maastricht Treaty (TEU)

On 25 March 1957 the six founder members of the European Economic Community had signed the Treaty Establishing the European Economic Community (also known as the Treaty

[31] See: *Lord Ashcroft v AG* [2002] EWHC 1122 (QB).

[32] *R v Brown* [1996] 1 All ER 545 at 555-556 (Lord Hoffmann).

[33] *Report of a Committee on Privacy and Related Matters*, chaired by Sir David Calcutt QC (Cm 1102). It concluded that an overwhelming case for introducing a statutory tort of infringement of privacy had not so far been made out (§12.5). In 1992 Sir David Calcutt carried out a review of the Press Complaints Commission. In his report (Cm 2135, published in January 1993), he recommended that the Government should give further consideration to the introduction of a tort of infringement of privacy. In July 1993 the Lord Chancellor's Department and the Scottish Office issued a consultation paper called Infringement of Privacy, inviting responses on the proposal to create a tort of infringement of privacy. In July 1995 the Government published its response (Privacy and Media Intrusion, Cmnd 2918), concluding that no persuasive case had been made for statutory regulation of the press and announcing that it had no plans to introduce a statutory right to privacy.

CHAPTER 8

GDPR and DPA 2018: introduction

1. OVERVIEW

8– 001 Introduction

With effect from 25 May 2018, the legislative regime in the United Kingdom governing data protection ceased to be Directive 95/46/EC and the DPA 1998 and became the GDPR, the Law Enforcement Directive ('the LED')[1] and the DPA 2018.[2] The GDPR is a regulation of the European Parliament and of the Council.[3] Being a regulation of the EU, the GDPR is directly

[1] Directive 2016/680.

[2] GDPR Art 99(2); DPA 2018 s 212; Data Protection Act 2018 (Commencement No 1 and Transitional and Saving Provisions) Regulations 2018 (SI 2018/625) reg 2.

[3] The source of the power to make the GDPR is Art 16 of the TFEU, which provides:
'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.

applicable in Member States.[4] A regulation does not always require a Member State to pass legislation to give its provisions legal effect within that Member State. A regulation may, however, contain provisions empowering each Member State to pass its own implementing measures or conferring on each Member State legislative latitude – which may be limited to derogations – on specific aspects covered by the regulation.[5] The GDPR adopted the permissive approach, conferring on each Member State a considerable degree of legislative latitude on a range of matters covered by it.[6]

8– 002 The new regime

Under the new regime, the processing of personal data in the United Kingdom is divided into four separate regulatory sectors:

(1) Intelligence services processing of personal data. This sector is governed by Part 4 of the DPA 2018 (ss 82-108). The GDPR has no role. This is dealt with in Chapters 8 and 14.

(2) Processing of personal data by competent authorities for law enforcement purposes. This is governed by Part 3 of the DPA 2018 (ss 29-81), which implements the LED in the United Kingdom. The GDPR has no role. This sector is dealt with in Chapters 8, 12 and 13.

Processing of personal data that is not within (1) or (2) is termed 'general processing.' There are two separate sectors dealing with general processing:

(3) Processing of personal data that falls within the GDPR.[7] This sector is governed by the GDPR as supplemented by Chapters 1-2 of Part 2 of the DPA 2018 (ss 4-20). This is dealt with in Chapters 8-11.

(4) Processing of personal data that falls outside the GDPR. The GDPR has no direct role, but it is applied with modifications by Chapter 3 of Part 2 of the DPA 2018 (ss 21-28). This sector, too, is dealt with in Chapters 8-11.

Most processing of personal data within the United Kingdom is general processing and falls within the third of the above sectors. It follows that the GDPR, as supplemented by the DPA 2018, governs most processing of personal data in the United Kingdom.

8– 003 Objectives of the GDPR

The objectives of the GDPR are stated to be:

> ...to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the [European] Union[8]

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.'

4 TFEU Art 288. By contrast, a directive, such as 95/46/EC, while binding as to the result to be achieved and requiring the Member State to legislate within a prescribed period to give effect to the directive, leaves to each Member State the choice of the most suitable form and method of doing so. Upon incorporation into the EEA Agreement (6 July 2018), the GDPR became applicable in Iceland, Liechtenstein and Norway.

5 These are often termed 'opening clauses.'

6 See especially GDPR Art 23(1) (restricting the rights of data subjects in certain circumstances), but also Arts 4(7) (definition of 'controller'), 6(2) (allowing a Member State to determine when processing is necessary in the public interest or to carry out a statutory function), 8(1), 9(2)(a), (g), (h), (i), (j), 9(4), 10, 14(5)(c), 17(1)(e), 17(3)(b), 18(2), 22(2)(b) (allowing a Member State to limit controls on automated decision-making and profiling), 26(1), 28(3)(a), (g), 29, 32(4), 35(10), 36(5), 37(4) (dealing with data protection officers), 38(5) and 88 (data processing under employment contracts).

7 The GDPR applies to personal data processed by automated means and, where personal data is processed by other than automated means, where the personal data forms part of a filing system. As to the meaning of these terms, see §§8– 040 to 8– 041.

8 GDPR recital (166).

and

> to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the [European] Union[9]

Article 1 of the GDPR further provides for its subject-matter and objectives:

> 1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
> 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
> 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

The GDPR is thus the confluence of two objectives: the rights and freedoms of natural persons to the protection of their personal data;[10] and the removal of impediments to the free movement of the personal data. Notably, the GDPR aims to ensure a 'high'[11] level of protection for the former. Those fundamental rights and freedoms are enshrined in Article 8(1) of the Charter of Fundamental Rights[12] and in Article 16(1) of the TFEU.[13]

8– 004 Continuing obligations

The GDPR imposes on each 'controller'[14] a continuing obligation to comply with six principles relating to the processing of personal data:[15]

(1) Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject – 'lawfulness, fairness and transparency.'[16]

(2) Personal data shall be collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes – 'purpose limitation.'[17]

(3) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed – 'data minimisation.'[18]

(4) Personal data processed shall be accurate and, where necessary, kept up to date – 'accuracy.'[19]

(5) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed – 'storage limitation.'[20]

(6) Personal data shall be 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

---

9 GDPR recital (170).

10 As to the meaning of 'rights and freedoms of natural persons' in this context, see §8– 006.

11 GDPR recitals (6) and (10).

12 As to which, see §§7– 019 to 7– 023.

13 As to which, see §7– 025.

14 The equivalent of the 'data controller' in the DPA 1998. As to the meaning of 'controller,' see further §8– 019.

15 GDPR Art 5.

16 Considered further at §§9– 006 to 9– 022.

17 Considered further at §§9– 023 to 9– 027.

18 Considered further at §9– 028.

19 Considered further at §§9– 029 to 9– 030.

20 Considered further at §§9– 031 to 9– 033.

organisational measures – 'integrity and confidentiality.'[21]

The obligation to comply with these six processing principles is called 'accountability.'[22] In addition to the obligation to comply with these processing principles, there are three other sets of continuing obligations which may or may not arise according to the type of processing being carried out and to the type of organisation that is the controller or processor:

- Additional obligations imposed on a controller processing sensitive personal information.[23]
- Obligations relating to the set up and internal organisation of a controller or processor.[24] These depend on the size of the controller or processor.
- Obligations engaged by the international transfer of personal data.[25]

Non-compliance with, or an inability to demonstrate compliance with, any of these obligations exposes the controller both to regulatory action (through the Information Commissioner)[26] and to a private law claim from the individual to whom the personal data relates.[27]

8– 005 Data subject rights

In addition to the continuing obligations, the GDPR confers on every individual seven conditional rights in respect of processing of his or her personal data, all but one of which is engaged by the individual giving a notice to the controller, who then becomes subject to a correlative obligation to comply with that notice:[28]

(1) A right of access, which comprises confirmation by the controller whether or not personal data concerning the data subject are being processed and, if so, being informed of the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data have been or will be disclosed, the period for which the personal data will be stored, the source of the data (if it is not the data subject) and certain other information.[29]

(2) A right of rectification, which comprises the right to obtain from a controller rectification of inaccurate personal data concerning the data subject, including completion of incomplete personal data.[30]

(3) A right of erasure (sometimes termed 'the right to be forgotten'), which comprises the right to obtain from a controller the erasure of personal data concerning the data subject.[31]

(4) A right to restrict processing (other than storage) of personal data.[32]

(5) A right to data portability, which comprises a right to receive personal data relating to the data subject in a machine-readable format and the right to transmit that data

---

21 Considered further at §§9– 034 to 9– 039.

22 GDPR Art 5(2) and recital (85).

23 Considered further at §§9– 040 to 9– 047. As to the meaning of 'sensitive personal information' see §9– 040.

24 Considered further at §§9– 048 to 9– 056.

25 Considered further at §§9– 057 to 9– 064.

26 GDPR Art 77. Regulatory enforcement is considered at §§48– 014 to 48– 055.

27 GDPR Art 79. Private law claims are considered at §§48– 005 to 48– 013.

28 GDPR Art 12. The exception is the right against automated decision-making. This does not require a notice but subsists whenever a controller is processing the personal data of a data subject.

29 GDPR Art 15. Considered further at §§10– 014 to 10– 017.

30 GDPR Arts16 and 19. Considered further at §§10– 018 to 10– 022.

31 GDPR Arts 17 and 19. Considered further at §§10– 023 to 10– 028.

32 GDPR Arts18 and 19. Considered further at §§10– 029 to 10– 034.

to another controller.[33]

(6) A right to object to processing of a data subject's personal data and to compel cessation of that processing.[34]

(7) A right to prevent automated decision-making, including profiling.[35]

Non-compliance with the obligation triggered by engagement of the right exposes the controller both to regulatory action and to a private law claim from the individual.[36]

8– 006 Rights and freedoms of persons

The original treaties of the European Economic Community did not contain any references to fundamental rights and their protection.[37] As the objectives of the EEC were primarily economic, it was unnecessary to do so. Moreover, the ECHR appeared to offer adequate protection. However, the CJEU gradually absorbed elements from various international treaties, including the ECHR, to produce a body of 'fundamental rights and freedoms' upon which it asserted the Community legal order was premised. From this stems the characterisation of the central objective of the GDPR – like Directive 95/46/EC before it[38] – namely, to protect fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.[39] This central objective is now independent of, and is not coincident with, the right to the protection of personal privacy. Although a set of facts and circumstances may contravene both the right to privacy and the right to the protection of personal data, the obligations imposed and rights conferred by the GDPR do not turn on there being a breach of personal privacy.[40] The existence of an individual's right to the protection of personal data concerning him or her that is separate from the right to respect for an individual's private and family life, home and communication – which embodies a right to personal privacy that includes personal information[41] – is acknowledged in the Charter.[42] The

---

33 GDPR Art 20. Considered further at §§10– 035 to 10– 039.

34 GDPR Art 21. Considered further at §§10– 040 to 10– 044.

35 GDPR Art 22. Considered further at §§10– 045 to 10– 048.

36 GDPR Arts 77 and 79. Regulatory enforcement is considered at §§48– 014 to 48– 055. Private law claims are considered at §§48– 005 to 48– 013.

37 See further §7– 018.

38 Directive 95/46/EC had used the same phrase and balancing device, expressly recognising 'the right to privacy' as one of those rights and freedoms: see Arts 1(1), 7(f), 18(2), 20(1), 28(4) and 30(1)(c) and recitals (2), (7), (8), (9), (10), (11), (30), (46), (49), (53) and (68). That Directive expressly linked 'rights and freedoms' of natural persons to the ECHR Art 8 and general principles of Community law and to Convention 108: see recitals (10) and (11) respectively.

39 GDPR Art 1(2). The centrality of protecting fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data is borne out by the repeated reference to this concept in the GDPR recitals: see (2), (9), (10), (16), (47), (51), (54), (68), (69), (73)-(81), (84)-(86), (89), (91), (94), (98), (113), (137), (156), (162), (166) and (173). And see also: *Google Spain SL v Agencia Espanola de Proteccion de Datos* (C-131/12) [2014] QB 1022 at [53]; *Puškár v Finančné riaditeľstvo Slovenskej* (C-73/16) [2017] 4 WLR 209, [2018] 1 CMLR 44 at [38]; *Buivids v Latvia* (C-345/17) [2019] 1 WLR 4225, [2019] 2 CMLR 24 at [45]; *Tietosuojavaltuutettu v Jehovan todistajat* (C-25/17) [2019] 4 WLR 1, [2019] 1 CMLR 5 at [35]; *Unabhangiges Landeszentrum fur Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) [2018] 3 CMLR 32, [2019] 1 WLR 119 at [87]; *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (C-40/17), CJEU, 29 July 2019 at [50].

40 The GDPR does not once use the word 'privacy.' In this way, the protection afforded by the GDPR may be seen to be more extensive than that afforded by ECHR Art 8 (which, in this sphere, is concerned with the protection of personal privacy).

41 And similarly under ECHR Art 8, see for example: *Klass v Germany* (1979-80) 2 EHRR 214 (interception of communications); *A v France* (1993) 17 EHRR 462 (interception of telephone); *Peck v United Kingdom* (2003) 36 EHRR 41, 13 BHRC 669 (CCTV images); *Perry v United Kingdom* (2003) 39 EHRR 76 (covert surveillance at police station during interview with montage); *Rotaru v Romania* (2000) 8 BHRC 449 (retention of old surveillance records); *Z v Finland* (1997) 25 EHRR 371 (uninvited disclosure of medical records); *Malone v United Kingdom* (1985) 7 EHRR 14 (interception of mail and telephone and numbers called); *Szabo v Hungary* (2016) 63 EHRR 102 (legislation permitting personal surveillance); *Big Brother Watch v United Kingdom* [2018] ECHR 58170/13 (retention of personal

GDPR repeatedly uses this conception of the rights and freedoms of the individual, embodying the right to the protection of personal data, as a touchstone by which to measure the acceptability of specific issues and measures in the processing of personal data.[43]

8– 007 Risks to rights and freedoms

Many of the obligations imposed on controllers and processors by the GDPR involve a consideration of 'risks' to the 'rights and freedoms of natural persons,' with those rights and freedoms including their right to the protection of personal data.[44] The risks to those rights and freedoms from processing include physical, material and non-material damage.[45] Such damage expressly includes:

- resultant discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable natural persons, in particular of children, are processed; and
- where processing involves a large amount of personal data and affects a large number of data subjects.[46]

The 'risk' to the rights and freedoms of natural persons is the combination of the severity of impact of an occurrence upon the rights and freedoms of natural persons and the likelihood of that occurrence. Risk is to be measured on the basis of an objective assessment.[47]

8– 008 European Data Protection Board

data for law enforcement purposes); *In re Gallagher* [2019] UKSC 3, [2019] 2 WLR 509 (disclosure of spent convictions to employer); *Segerstedt-Wiberg v Sweden* (2006) 44 EHRR 14, 21 BHRC 155 at [72] (information recording participation of an individual at a public demonstration); *MM v United Kingdom* [2012] ECHR 1906 at [188] (record of conviction); *B v General Medical Council* [2018] EWCA Civ 1497, [2019] 2 All ER219 (professional criticism of individual); *R (C) v Secretary of State for Work and Pensions* [2017] UKSC 72, [2017] 1 WLR 4127 (computer record of individual's gender history). But contrast: *In Re JR38* [2015] UKSC 42, [2016] AC 1131.

[42] As to the Charter, see further §§7– 019 to 7– 033. It is for this reason that the authorities speak of the fundamental rights (plural) to privacy and to the protection of personal data: *GC v Commission nationale de l'informatique et des liberté* (C-136/17) [2019] All ER (D) 66 (Sep) at [37], [44], [46], [59], [67], [68]; *Tietosuojavaltuutettu v Jehovan todistajat* (C-25/17) [2019] 4 WLR 1, [2019] 1 CMLR 5 at [18]; *Puškár v Finančné riaditeľstvo Slovenskej* (C-73/16) [2017] 4 WLR 209, [2018] 1 CMLR 44 at [30]; *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15) [2017] QB 771, [2017] 2 CMLR 30 at [93].

[43] GDPR Arts 5(1)(e), 6(1)(f), 9(2)(i), 10, 14(5)(b), 15(4), 20(4), 21(1), 22(2)(b), (3), (4), 23(1), (2), 24(1), 25(1), 27(2)(a), 30(5), 32(1), 33(1), 34(1), (3)(b), 35(1), 35(7)(c), 36(3)(c), 49(1), 50(b), 51(1), 57(1)(c), 66(1), (3), 80(1), 87, 88(1) and 89(1).

[44] GDPR Art 1(2) and recitals (2) and (9).

[45] GDPR recital (75).

[46] GDPR recital (75).

[47] GDPR recital (76).

Up to 25 May 2018 the Article 29 Working Party – 'Art 29 WP' – had been the independent European working party that dealt with issues relating to the protection of privacy and personal data. It was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The Art 29 WP produced various working papers that dealt with issues arising in data protection. On 25 May 2018, with the coming into force of the GDPR, the Art 29 WP was replaced by the European Data Protection Board – 'the EDPB.' During its first plenary meeting the EDPB endorsed all of the Art 29 WP working papers, which serve as guidance on the operation of the GDPR.

8– 009 DPA 2018

The DPA 2018 supplements the processing of personal data that is covered by the GDPR, implements the Law Enforcement Directive – the LED – in the UK, and deals with processing of personal data that is not covered by the GDPR. The combined effect of the DPA 2018 and the GDPR is to create a regime that covers the field of data protection in the United Kingdom. In summary, the DPA 2018 splits the field of data protection into four sectors, each of which it treats separately. Starting with the most specific, these four sectors are:

(1) Processing of personal data by the intelligence services – 'intelligence services processing.' This is a topic that is not within the legislative competence of the EU legislator, hence not covered by either the GDPR or the LED. The principal provisions dealing with processing of personal data by the intelligence services are in Part 4 of the DPA 2018 (ss 82-108). This is the sector in which an individual's rights are most abbreviated and, correlatively, the controller is most free to process personal data without legislative constraint.[48]

(2) Processing of personal data by competent authorities for law enforcement purposes – 'law enforcement processing.' The GDPR is inapplicable to this processing. The principal provisions in the DPA 2018 dealing with this processing are in Part 3 (ss 29-81). These provisions represent the domestic implementation of the LED, which was required to be transposed into domestic law by 6 May 2018.[49] Although an individual's rights are abbreviated, their reduction is not as marked as in relation to processing of personal data by the intelligence services.[50]

(3) General processing (ie processing that is not within (1) or (2) above) that:

  (a) is outside the scope of EU law; and

  (b) that is processing by a Member State when carrying on an activity that falls within the EU's common foreign and security policy,[51]

or that involves processing by a public authority without using automated means or a filing system – 'applied GDPR processing.' For this processing, the DPA 2018 applies a modified GDPR, which it terms the 'applied GDPR.'[52] The principal provisions are ss 21-28 of the DPA, together with the applicable Schedules.[53]

(4) Processing governed by the GDPR: in other words, all processing of personal data not within (1), (2) or (3) above – 'general processing.' As previously noted, most processing of personal data falls within this sector. In this sector, the DPA 2018 exercises for the United Kingdom the legislative latitude conferred on each Member

[48] See Chapter 14.

[49] LED Art 63.

[50] See Chapters 12-13.

[51] That is, within Chapter 2 of Title V of the TEU: see GDPR Art 2(2)(b).

[52] DPA 2018 s 3(11).

[53] See Chapters 9-11.

State by the GDPR. The Act does not displace, supplant or override the GDPR. To the extent that processing of personal data is governed by the GDPR, the DPA 2018 supplements, and must be read with, the GDPR.[54] The principal provisions are ss 4-20 of the DPA 2018, together with the applicable Schedules. In practice, for most controllers that are not public authorities, general processing covered by the GDPR will be the only processing with which they will be concerned.[55]

Collectively, the four sectors may be called 'the data protection regime.' The DPA 2018 also deals with the Information Commissioner and with the enforcement – by the Information Commissioner and the courts – of the GDPR and DPA 2018.[56]

2. TERMINOLOGY

8– 010 Introduction

As with the DPA 1998, the data protection regime employs a number of key terms that are critical to an understanding of its operation:

- The *individual* whose interests are protected by the regime is the 'data subject,' who is an 'identified or identifiable natural person.'
- The *activity* regulated by the regime is called 'processing.'
- The *matter* the processing of which is regulated by the regime is called 'personal data,' being 'information relating to' a data subject.
- The principal *person* whose activity is regulated by the regime is called the 'controller.'[57] This is the person who determines the processing carried out on the personal data. A lesser degree of regulation is imposed on a 'processor,' being the person who processes personal data as instructed by the controller.
- The *standard* of processing required by the regime is prescribed by a set of continuing 'obligations' which persist throughout the processing. The obligations include adherence to a set of 'processing principles.'
- A data subject has *rights* which, apart from enforcing adherence to the obligations and requirements in relation to automated decision-making, are triggered by giving notice to the controller.

The definition given to these and other terms varies according to the applicable regulatory sector: that is, whether the processing in question constitutes 'general processing,' 'law enforcement processing,' or 'intelligence services processing.' In addition, within each of the four sectors certain terminology is used that is unique to that sector. The terms considered below are common to two or more of the sectors, with any differences footnoted. Terminology that is unique to a particular sector in the relevant chapter.[58]

8– 011 Identified or identifiable persons

The obligations imposed and the rights conferred by the data processing regime are imposed and conferred for the benefit of 'identified or identifiable natural persons' only.[59] Accordingly,

---

[54] DPA 2018 s 4(2)(b).

[55] See Chapters 9-11.

[56] DPA 2018 Parts 5 and 6.

[57] Called the 'data controller' in the DPA 1998.

[58] In relation to law enforcement processing, see §§12– 006 to 12– 010. In relation to intelligence services processing, see §§14– 002 to 14– 003.

[59] GDPR Art 4(1) and recital (26) and DPA s 3(5), applying to all sectors. This is also the approach taken in Convention 108 Mod. A different approach is taken by the ePrivacy Directive, Art 1(2) and recital (7).

CHAPTER 48

GDPR and DPA 2018: private remedies and regulatory enforcement

1. OVERVIEW

48– 001 Introduction

To make effective the applicable data processing requirements, the GDPR and the DPA 2018 enable a data subject to seek from a court private remedies against a contravening controller or processor, as well as enabling the Information Commissioner to undertake regulatory enforcement against a contravening controller or processor. A single breach of a requirement in the GDPR or the DPA 2018 may expose a controller or processor to both private remedies and regulatory enforcement, with the latter able to complement the former. A breach of a code of practice issued by the Information Commissioner does not of itself give rise to a private remedy, although it may be relied upon to initiate regulatory enforcement.[1] Regulatory enforcement may be instigated on the Information Commissioner's own motion or on a complaint by a data subject.[2] The scope of the remedies and regulatory enforcement that are available upon non-compliance with the requirements of the data protection regime depends upon whether the processing is by one of the intelligence services, by a competent authority for law enforcement purposes or whether it is general processing.[3]

48– 002 Private remedies

The remedies that are available to a data subject depend upon:

- the particular continuing obligation or data subject right that has not been complied with;
- the consequences of non-compliance for the data subject;
- whether in relation to the processing for which a remedy is sought, the person against whom that remedy is sought is the controller or a processor of the personal data; and
- whether the processing is by one of the intelligence services, by a competent authority for law enforcement purposes or whether it is general processing.

The private remedies divide into:

- compliance remedies, where an order is sought that the defendant controller or processor be compelled to carry out specified remedial action within a prescribed time; and
- compensatory remedies, where an award of money is sought to compensate the data subject for a contravention of a right or principle.

A single claim may seek both types of remedy.

48– 003 Regulatory enforcement

The Information Commissioner is responsible for regulatory enforcement under both the GDPR and the DPA 2018.[4] Where a data subject makes a complaint to the Commissioner, the Commissioner must investigate the subject matter of the complaint and inform the data

---

1 DPA 2018 s 127(2), (4). Nevertheless, a court or tribunal must, in any proceedings before it, take into account any relevant code of practice in force at the relevant time: DPA 2018 s 127(3). Similarly, a breach of the Framework for Data Processing by Government prepared under DPA 2018 s 191 does not of itself give rise to a private remedy, but is to be taken into account by a court or tribunal in any proceedings before it: DPA 2018 s 194.

2 DPA 2018 s 165(1)-(2).

3 On the division between processing by 'the intelligence services,' a 'competent authority for law enforcement purposes' and 'general processing', see further §8– 002.

4 DPA 2018 ss 115-116; GDPR Arts 51, 57 and 58; LED Art 41.

subject of the outcome of that complaint.[5] The principal enforcement measures that may be taken by the Information Commissioner are:

(1) Issuing an information notice against either a controller or a processor or any other person.[6] An information notice will require the recipient to provide the Commissioner with particular information, or a category of information, that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation.[7]

(2) Issuing an assessment notice against either a controller or a processor.[8] An assessment notice permits the Information Commissioner to assess whether the controller or processor has complied or is complying with the data protection legislation. An assessment notice may require a controller or a processor to permit the Commissioner to enter premises, to direct the Commissioner to particular documents, to assist the Commissioner to view documents, to provide copies of them, to direct the Commissioner to equipment or other material on the premises, to permit the Commissioner to inspect documents, information, equipment or material and to provide the Commissioner with an explanation of them, to permit the Commissioner to observe the processing of personal data and to make available for interview persons who process personal data on behalf of the controller.[9]

(3) Issuing an enforcement notice against a controller or processor.[10] An enforcement notice may be issued against a controller or processor where it has failed, or is failing, to comply with its continuing obligations or with a data subject's rights.[11] An enforcement notice will impose requirements that the Commissioner considers appropriate for the purpose of remedying the failure.[12] In this way, an enforcement notice may be used to achieve the same outcome as private proceedings brought by a data subject seeking compliance remedies.

---

5 GDPR Arts 57(1)(f) and 77(2) (general processing); DPA 2018 s 165(5)-(6) (law enforcement processing and intelligence services processing). Where the Information Commissioner fails to take appropriate steps or fails to inform the data subject of the outcome of the complaint within 3 months of receipt, the data subject may apply to the First-tier Tribunal for an order requiring the Commissioner to take appropriate steps or to inform the data subject of the outcome within a specified time: DPA 2018 s 166. Provided that the Information Commissioner informs the data subject about the progress of the complaint within 3 months of receipt, the Commissioner is given a further three months within which to inform the data subject of the outcome: DPA 2018 s 166(1).

6 DPA s 142(1); in relation to general processing, see also GDPR Art 58(1)(a) and DPA 2018 s 115(5). In relation to intelligence services processing, the power to issue an information notice is disapplied where that is required for the purpose of safeguarding national security: DPA 2018 s 110. The Commissioner may not give an information notice with respect to the processing of personal data for 'the special purposes' other than in very limited circumstances: DPA 2018 s 143(1). As to the meaning of 'the special purposes' see §11– 050.

7 The 'data protection legislation' means the GDPR, the applied GDPR, the DPA 2018 and regulations thereunder, and regulations made under the European Communities Act 1972 s 2(2) that related to the GDPR or the LED: DPA 2018 s 3(9).

8 DPA 2018 s 146(1); in relation to general processing, see also GDPR Art 58(1)(b) and DPA 2018 s 115(6). In relation to intelligence services processing, the power to issue an assessment notice is disapplied where that is required for the purpose of safeguarding national security: DPA 2018 s 110.

9 DPA 2018 s 146(2).

10 DPA 2018 s 149(1); in relation to general processing, see also GDPR Art 58(1)(c)(g), (j) and (h) and DPA 2018 s 115(8). In relation to intelligence services processing, the power to issue an enforcement notice is disapplied where that is required for the purpose of safeguarding national security: DPA 2018 s 110. Enforcement notices may also be issued against a monitoring body that has failed or is failing to comply with an obligation under GDPR Art 41 and against a certification provider: DPA 2018 s 149(3)-(4). The Commissioner may not give an enforcement notice with respect to the processing of personal data for 'the special purposes' other than in very limited circumstances: DPA 2018 s 152(1). As to the meaning of 'the special purposes' see §11– 050.

11 DPA 2018 s 149(2). This also lists other circumstances in which an enforcement notice may be issued against a controller or processor.

12 DPA 2018 s 149(6).

(4) Issuing a penalty notice against a controller or processor where it has failed, or is failing, to comply with its continuing obligations or with a data subject's rights,[13] or where there has been a failure to comply with an information notice, an assessment notice or an enforcement notice.[14]

There is a right of appeal against each of these types of notice.

48– 004 Data subject complaints

A data subject has a statutory right to complain to the Information Commissioner if the data subject considers that, in relation to personal data relating to him or her, there has been an infringement of the requirements of data protection legislation.[15] This includes an infringement of any of the continuing obligations or any of the data subject rights.[16] Where the Commissioner receives such a complaint, the Commissioner must:

(a) take appropriate steps to respond to the complaint, including investigating and responding to it;
(b) inform the complainant of the outcome of the complaint;
(c) inform the complainant of the right to apply to the First-tier Tribunal for an order requiring the Commissioner to progress the complaint and inform the complainant of the progress and outcome of it; and
(d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.[17]

If the Commissioner does not take appropriate steps to respond to it or, within three months of having received the complaint, has not provided the complainant with information about progress (or the outcome) of the complaint, the complainant may apply to the First-tier Tribunal for an order requiring the Commissioner to take, within a specified period, appropriate steps to respond to the complaint or to inform the complainant of progress or the outcome of the complaint.[18]

---

[13] DPA 2018 s 155(1)(a); in relation to general processing, see also GDPR Arts 58(2)(i) and 83 and DPA 2018 s 115(9). In relation to intelligence services processing, there is no disapplication of the Information Commissioner's power to issue a penalty notice on the grounds of safeguarding national security: DPA 2018 s 110(2)(e)(i).

[14] DPA 2018 s 155(1)(b); in relation to general processing, see also GDPR Arts 58(2)(i) and 83 and DPA 2018 s 115(9). In relation to intelligence services processing, there is no disapplication of the Information Commissioner's power to issue a penalty notice on the grounds of safeguarding national security: DPA 2018 s 110(2)(e)(i). The Commissioner may not give a penalty notice with respect to the processing of personal data for 'the special purposes' other than in very limited circumstances: DPA 2018 s 156(1). As to the meaning of 'the special purposes' see §11– 050.

[15] GDPR Art 77 (general processing); DPA 2018 s 165(1)-(2) (law enforcement processing and intelligence services processing). As well as being made by a data subject him or herself, the complaint may be made on behalf of a data subject by a body or association that is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data provided that that body or associates is required to apply all of its income and capital for charitable purposes, is prohibited from directly or indirectly distributing amongst its members any part of its assets (other than for charitable purposes) and has objectives that are in the public interest – called a 'representative body': GDPR Art 80 (in relation to general processing); DPA 2018 s 187 (in relation to law enforcement processing and intelligence services processing).

[16] The continuing obligations are the obligations set out in Chapter 9 (in relation to general processing), Chapter 12 (in relation to law enforcement processing) and Chapter 14 (in relation to intelligence services processing). The data subject rights are those set out in Chapter 10 (in relation to general processing), Chapter 13 (in relation to law enforcement processing) and Chapter 14 (in relation to intelligence services processing).

[17] GDPR Arts 57(1)(f) and 77(2) (in relation to general processing); DPA 2018 s 165(4)-(5) (in relation to law enforcement processing and intelligence services processing).

[18] DPA 2018 s 166(1)-(2). If the Commissioner's consideration of the complaint is not concluded within 3 months, the Commissioner must, within each 3 months period until conclusion of the investigation, provide the complainant with information about progress of the complaint: DPA 2018 s 166(1). The application may be made to the FTT by a representative body on behalf of the data subject: GDPR Art 80 (in relation to general processing); DPA 2018 s 187(2)(b) (in relation to law enforcement processing and intelligence services processing).

2. PRIVATE REMEDIES

48– 005 Introduction

All three types of data processing – that is, general processing, law enforcement processing and intelligence services processing – provide data subjects with private law remedies of varying scope. The potential remedies are coercive – called a 'compliance order'[19] – and compensatory.

48– 006 Nature of the claim

In the taxonomy of private law claims, a claim by a data subject that a controller or processor, in processing his or her personal data, has not-complied with one or other of its continuing obligations[20] or the data subject's rights[21] is a claim in tort – namely, the tort of breach of statutory duty. As such, the limitation period is:

(a) Where the damages claimed consist of or include damages in respect of personal injuries[22] to the claimant or any other person – 3 years from the later of the date on which the cause of action accrued or the date of knowledge of the person injured.[23]

(b) Otherwise – 6 years from the date on which the cause of action accrued.[24]

To the extent that a claim involves a foreign element the Private International Law (Miscellaneous Provisions) Act 1995 means that the assessment of damages will be determined in accordance with the law of England and Wales.[25]

48– 007 Jurisdiction

Private remedies are claimed in the civil courts, and not in the tribunals.[26] In relation to claims arising out of processing by a competent authority for law enforcement purposes and in relation to claims arising out of general processing, jurisdiction is exercisable by the High Court or a county court (in England, Wales and Northern Ireland) and by the Court of Session or the sheriff (in Scotland).[27] The choice between the High Court and the county court will be decided on the usual principles.[28] The High Court (in Scotland, the Court of Session) has

---

[19] DPA 2018 s 167. A controller may be vicariously liable for employee breaches: *WM Morrisons plc v Various Claimants* [2020] UKSC 12 at [54]-[55].

[20] That is, the obligations set out in Chapter 9 (in relation to general processing), Chapter 12 (in relation to law enforcement processing) and Chapter 14 (in relation to intelligence services processing).

[21] That is, the data subject rights set out in Chapter 10 (in relation to general processing), Chapter 13 (in relation to law enforcement processing) and Chapter 14 (in relation to intelligence services processing).

[22] 'Personal injuries' includes any disease and any impairment of a person's physical or mental condition: Limitation Act 1980 s 38(1).

[23] Limitation Act 1980 s 11(4). Date of knowledge is determined in accordance with Limitation Act 1980 s 14. A failure to notify a data subject of the right to apply to a court under DPA 2018 s 167 may be relevant for this purpose: see DPA 2018 s 44(5), 45(5), 48(1) and 51(5).

[24] Limitation Act 1980 s 2. As damage is not necessary to bring a data protection claim, the cause of action will accrue from the date on which the breach occurred: Limitation Act 1980 s 2. Where a defendant has deliberately concealed from a claimant any fact relevant to the claimant's right of action, the period of limitation will not begin to run until the claimant has discovered the concealment or could with reasonable diligence have discovered it: Limitation Act 1980 s 32(1).

[25] Private International Law (Miscellaneous Provisions) Act 1995 s 14(3)(b). The Rome II Regulation does not apply: see Art 1(2)(g).

[26] DPA 2018 s 20.

[27] DPA 2018 s 180(1); GDPR Arts 79(2) and 82(6).

[28] In England and Wales, the default position is that proceedings (whether for damages or for a specified sum) may not be started in the High Court unless the value of the claim is more than £100,000: CPR PD7A para 2.1. This

exclusive jurisdiction to hear claims arising out of processing of personal data by the intelligence services.[29]

48– 008 Pre-action practice: claimant

Before a claim is issued in the High Court, the pre-action protocol for media and communication claims should be followed.[30] This requires a claimant to give the defendant written notification of the claim – a 'letter of claim' – at the earliest opportunity, setting out the name of the claimant, the nature and basis for the entitlement to the remedies sought, any facts or matters relevant to England and Wales being the most appropriate forum for the dispute, and details of any funding arrangement in place.[31] In addition, the letter of claim should include the following information:

(a) any further information necessary to identify the data subject;
(b) the data controller to which the claim is addressed;
(c) the information or categories of information which is claimed to constitute personal data including, where necessary, the information which is said to constitute sensitive personal data or to fall within a special category of personal data;
(d) sufficient details to identify the relevant processing;
(e) the identification of the duty or duties which are said to have been breached and details of the manner in which they are said to have been breached, including any positive case on behalf of the claimant;
(f) why the personal data ought not to be processed/further processed, if applicable; and
(g) the nature and any available details as to any particular damage caused or likely to be caused by the processing or breach of duty complained of.[32]

Where a representative data protection claim is intended to be brought on behalf of data subjects, the letter of claim should also:

(h) set out the nature of the entity which intends to bring the claim and explain how it fulfils the relevant suitability criteria;
(i) include details of the data subjects on whose behalf the claim would be brought; and
(j) confirmation that they have mandated the representative body to represent them and receive compensation, where applicable.[33]

48– 009 Pre-action practice: defendant

is subject to the requirements of any enactment. In relation to data protection claims, the only such requirements are DPA 2018 ss 94(13), 99(7), 100(6) and 180(3) requiring claims arising out of processing of personal data by the intelligence services to be brought in the High Court (in Scotland, in the Court of Session). The default position will be displaced, with the effect that a claim for less than £100,000 should be started in the High Court, where by reason of—
(1) the financial value of the claim and the amount in dispute, and/or
(2) the complexity of the facts, legal issues, remedies or procedures involved, and/or
(3) the importance of the outcome of the claim to the public in general,
the claimant believes that the claim ought to be dealt with by a High Court judge: PD7A para 2.4.

29 DPA 2018 ss 94(13), 99(7), 100(6) and 180(3).

30 The extent to which the protocol has been followed by the parties will be taken into account by a court in dealing with liability for costs and making other orders: Protocol para 1.3. The Protocol applies to cases within the scope of CPR r 53.1, but this does not extend to data protection claims initiated in the County Court unless the claim arises from activities of the media: see Protocol para 1.1 and the definition of 'media and communications claim' in CPR r 53.1.

31 Protocol para 3.1.

32 Protocol para 3.4. Where the letter of claim includes other causes of action, the protocol requirements for those causes should also be included.

33 Protocol para 3.4 and see GDPR Art 80.

The recipient of the letter of claim should provide a full response as soon as possible and, if more than 14 days is required, the recipient should immediately notify the claimant specifying the date by which the response will be provided.[34] The response should include the following:

(a) whether or to what extent the claimant's claim is accepted, whether more information is required or whether it is rejected;
(b) if the claim is accepted in whole or in part, the defendant should indicate which remedies it is willing to offer;
(c) if more information is required, then the defendant should specify precisely what information is needed to enable the claim to be dealt with and why;
(d) if the claim is rejected, then the defendant should explain the reasons why it is rejected, including a sufficient indication of any statutory exemptions or facts on which the defendant is likely to rely in support of any substantive defence; and
(e) where the claimant to a proposed action has indicated his or her intention to make an application to bring the claim anonymously, the defendant should indicate whether the defendant accepts such an order would be appropriate and give an indication of the basis for the defendant's position.[35]

48– 010 Court procedure

Where a claim initiated in the High Court includes allegations of a breach of the GDPR or the DPA 2018, that claim will fall within the definition of a 'media and communications claim' under the Civil Procedure Rules 1998.[36] A 'media and communications claim' must be issued in the Queen's Bench Division in the Media and Communications List.[37] In any 'media and communications claim' that includes allegations of breach of the GDPR or the DPA 2018, the claimant must specify in the particulars of claim:-

(a) the legislation and the provision that the claimant alleges the defendant has breached;
(b) any specific data or acts of processing to which the claim relates;
(c) the specific acts or omissions said to amount to such a breach, and the claimant's grounds for that allegation; and
(d) the remedies which the claimant seeks.[38]

48– 011 Representative actions etc

A single breach of the data protection principles may affect a group of data subjects. In relation to both general processing and law enforcement processing, special provision is made for a data subject to authorise certain bodies or other organisations to exercise the data subject's rights, both for compliance orders and for compensatory orders, as well as for a complaint to the Information Commissioner.[39] This is additional to the two procedures generally available in civil litigation for collective proceedings. There are thus three procedures potentially available for a breach of a data subject's rights to be brought by a claim other than in the data subject's own name:

---

[34] Protocol para 3.6.

[35] Protocol para 3.7.

[36] CPR r 53.1(2)-(3). This will include a claim that is issued in the High Court and transferred to the County Court under CPR 53.4(2).

[37] CPR rr 53.1(3)(b) and 53.4(1). This includes claims that also allege other causes of action, such as breach of confidence. See also para 19 of the Queen's Bench Guide.

[38] Practice Direction 53B para 9. Although this is only mandatory in relation to claims that must be made in Media and Communications List, it is good general practice.

[39] GDPR Art 80; LED Art 55; DPA 2018 ss 187-188.

(1) Representative proceedings.[40] Under the Civil Procedure Rules, where it is difficult or impossible for all persons affected by a claim to be parties to the proceedings, the court may order one or more persons to be made party to the claim as representative of persons who are not parties and to direct that orders made in the claim are to bind the represented persons. The critical requirement is that all the persons represented have 'the same interest' in the claim as the claimant. In a data protection claim, this will generally require the claim to be limited to one seeking compensation for the mere fact of a breach of the principles, rather than compensation that takes into account the particular circumstances of each of the data subjects.[41] It is not necessary for a representative claimant to obtain the authority of the represented person to bring the claim.[42] Nor is it necessary for a claimant to obtain the court's permission to issue a claim form as a representative of other claimants. A court has power to order that a person not act as a representative.[43] The representative claimant has full power to run the litigation on behalf of the represented class as the representative claimant thinks fit. Those represented are not parties to the litigation. Accordingly:

    (a) There is no disclosure against the represented parties, unless it is ordered as against a non-party.[44]

    (b) The represented parties are not liable for costs.[45]

(2) Under a group litigation order – a 'GLO.'[46] A GLO may be made where a number of claims give rise to common or related issues of fact or law. A GLO may be sought before or after the issue of a claim or claims. It may be sought by any party to a claim or on the court's own motion.[47] A GLO will identify the issues to be managed as part of the group litigation: for any individual claim to be captured by a GLO, it must raise these issues. It is a matter for the court to decide whether or not to make a GLO. Any judgment on a GLO issue will bind all the GLO claimants. Unlike representative proceedings, proceedings under a GLO allow for

---

40 Under CPR rr 19.6-19.7.

41 In *Lloyd v Google LLC* [2019] EWCA Civ 1599, [2020] EMLR 2, the claimant issued proceedings against the defendant Google on behalf of a class of more than 4 million Apple iPhone users, alleging that Google secretly tracked some of their internet activity, for commercial purposes, between 9 August 2011 and 15 February 2012. The claimant claimed a uniform amount by way of damages on behalf of each person within the defined class, without seeking to allege or prove any distinctive facts affecting any of them, save that they did not consent to the abstraction of their data. The judge at first instance had dismissed the claimant's application for permission to serve Google outside the jurisdiction inter alia on the basis that the members of the class did not have the 'same interest' within CPR 19.6(1) so as to justify allowing the claim to proceed as a representative action. This was overturned by the Court of Appeal on the basis that those whom the claimant sought to represent would all have had their browser generated information – something of value – taken by Google without their consent in the same circumstances during the same period, and were not seeking to rely on any personal circumstances affecting any individual claimant (whether distress or volume of data abstracted). The represented class were all victims of the same alleged wrong and had all sustained the same loss, namely loss of control over their browser generated information. The claimant had disavowed reliance on any facts affecting any individual represented claimant. That concession had the effect of reducing the damages that could be claimed to the lowest common denominator. Google could not raise any defence to one represented claimant that did not apply to all others. The wrong was the same and the loss claimed was the same. Therefore, the represented parties did, in the relevant sense, have the same interest. There was no injustice in the pleaded claim proceeding as a representative one (at [75]-[80]).

42 *Independiente Ltd v Music Trading On-line (HK) Ltd* [2003] EWHC 470 (Ch) at [32]; *Howells v Dominion Insurance Co Ltd* [2005] EWHC 552 (QB); *PNPF Trust Company Ltd v Taylor* [2009] EWHC 1693 (Ch) at [47].

43 CPR r 19.6(2).

44 *Ventouris v Mountain* [1991] 1 WLR 607, [1991] 3 All ER 472.

45 *Howells v Dominion Insurance Co Ltd* [2005] EWHC 552 (QB); *Smithkline Beecham plc v Avery* [2009] EWHC 1924 (QB).

46 Under CPR 19.11 and PD 19B.

47 PD 19B para 4.

divergences between the claimants: the judgment on the GLO issues leaves the other issues (eg quantification of compensation) to be decided on a claim-by-claim basis.

(3) Representation by a body or organisation pursuant to a data subject's authorisation.[48] This enables an individual data subject to authorise certain types of bodies or other organisations to exercise a data subject's rights, including the right to an effective judicial remedy. Unlike (1) and (2), there need be no other person apart from the single data subject with an interest in the claim or type of claim. In relation to non-General processing data protection claims, in order to be a 'representative body':

(a) by enactment or its constitution, the body must be required (after payment of outgoings) to apply the whole of its income any capital it expends for charitable purposes, it must be prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and it must have objectives that are in the public interest; and

(b) the body must be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.[49]

The Secretary of State may make regulations for a representative body to bring proceedings combining two or more such claims, but as yet no such regulations have been made.[50]

48– 012 Compliance orders

In relation to general processing and law enforcement processing (but not in relation to intelligence services processing),[51] where a court is satisfied that there has been an infringement of a data subject's rights under the data protection legislation in contravention of that legislation, it may make an order against the controller, or a processor acting on behalf of the controller, for the purposes of securing compliance with that legislation.[52] Such orders may be directed to non-compliance with the continuing obligations by a data controller or processor[53] or to a contravention of a data subject's rights.[54] A compliance order will require the controller, or a processor on behalf of that controller, to take the steps specified in that order or to refrain from taking the steps specified in that order, and it may specify the times within which each such step must be taken or desisted from.[55] The importance of compliance orders is

---

[48] As provided for in DPA 2018 ss 187-188; GDPR Art 80, recital (142); LED Art 55. Such a body or organisation is called a 'representative body': DPA 2018 s 187(5).

[49] DPA 2018 s 187(3)-(4) (in relation to law enforcement processing and intelligence services processing). In relation to General processing the requirements on the 'representative body' are substantially the same: GDPR Art 80(1).

[50] DPA 2018 s 188. This does not apply to Scotland.

[51] DPA 2018 s 167(4)(b). On the division between processing by 'the intelligence services,' a 'competent authority for law enforcement purposes' and 'general processing', see further §8– 002.

[52] DPA 2018 s 167(1). The 'data protection legislation' means the GDPR, the applied GDPR, the DPA 2018 and regulations thereunder, and regulations made under the European Communities Act 1972 s 2(2) that related to the GDPR or the LED: DPA 2018 s 3(9). In relation to general processing, DPA 2018 s 167(1) embraces the right to an effective remedy against a controller or processor provided for by GDPR Art 79(1): DPA 2018 s 167(4)(a).

[53] That is, the obligations set out in Chapter 9 (in relation to general processing) and Chapter 12 (in relation to law enforcement processing).

[54] That is, the data subject rights set out in Chapter 10 (in relation to general processing) and Chapter 13 (in relation to law enforcement processing).

[55] DPA 2018 ss 167(2)-(3).

underscored by the obligation on a controller to inform a data subject of the right to seek a compliance order.[56] In relation to intelligence services processing, a court may make the equivalent of a compliance order where:

(a) the controller has failed to comply with an access request;[57]
(b) the controller has not complied with a notice objecting to processing;[58]
(c) the personal data relating to the data subject is inaccurate;[59] or
(d) the processing infringes any of the six data protection principles applicable to intelligence services processing.[60]

48– 013 Compensatory orders

Any person who has suffered damage as a result of contravention of the data protection legislation is entitled to compensation from the controller or processor for the damage suffered.[61] This applies to all four types of processing. 'Damage' covers both material (eg financial loss) and non-material damage, including distress.[62] Any controller involved in the contravening processing will be liable for the damage so caused.[63] A processor will be liable only in respect of the contravention of obligations that are specifically directed to a processor or where the processor has acted outside or contrary to lawful instructions from the controller.[64] A controller or processor has a defence where it proves that it was not in any way responsible for the event giving rise to the damage.[65] In relation to general processing, where more than one controller or processor, or both a controller and a processor, are involved in the same processing and are responsible for any damage caused by the processing, their liability is joint and several.[66] In relation to law enforcement processing and intelligence services processing, joint controllers are required to have determined in advance their respective responsibilities in

---

56 GDPR Art 12(4) (in relation to general processing); DPA 2018 ss 44(5)(e), 45(5)(e), 48(1)(b)(iv), 48(4)(d) and 51(5) (in relation to law enforcement processing by a competent authority).

57 DPA 2018 s 94(11)-(12).

58 DPA 2018 s 99(4)-(7).

59 DPA 2018 s 100(1).

60 DPA 2018 s 100(2). As to the meaning of the six data protection principles applicable to intelligence services processing, see §§14– 007 to 14– 015. In relation to the breadth of the court's discretion to make or decline to make an order, see §14– 020.

61 GDPR Art 82(1) in relation to GDPR processing; DPA 2018 s 169(1) in relation to law enforcement processing and intelligence services processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(1) in relation to applied GDPR processing. On the division between 'intelligence services processing', 'law enforcement processing', 'GDPR processing' and 'applied GDPR processing', see §§8– 002 and 9– 002. The 'data protection legislation' means the GDPR, the applied GDPR, the DPA 2018 and regulations thereunder, and regulations made under the European Communities Act 1972 s 2(2) that related to the GDPR or the LED: DPA 2018 s 3(9).

62 GDPR Art 82(1) and DPA 2018 s 168(1) in relation to GDPR processing; DPA 2018 s 169(5) in relation to law enforcement processing and intelligence services processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(1) in relation to applied GDPR processing.

63 GDPR Art 82(2) in relation to GDPR processing; DPA 2018 s 169(2)(a) in relation to law enforcement processing and intelligence services processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(2) in relation to applied GDPR processing.

64 GDPR Art 82(2) in relation to GDPR processing; DPA 2018 s 169(2)(b) in relation to law enforcement processing and intelligence services processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(2) in relation to applied GDPR processing.

65 GDPR Art 82(3) in relation to GDPR processing; DPA 2018 s 169(3) in relation to law enforcement processing and intelligence services processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(3) in relation to applied GDPR processing.

66 GDPR Art 82(4) in relation to GDPR processing; DPA 2018 s 22(1) in conjunction with GDPR Art 82(4) in relation to applied GDPR processing. Where one or other has paid full compensation for the damage suffered, that controller or processor has a right of contribution from the other controller(s) or processor(s) according to the level of responsibility for the damage: GDPR Art 82(5).

a transparent 'arrangement.'[67] In those circumstances, a joint controller is only liable where that controller is responsible for compliance with the provision of the data protection legislation that has been contravened.[68] Damages awards under the previous data protection regime may provide some guidance to awards under the current regime, but the enlarged continuing obligations and data subject rights and the intervening recognition of a discrete fundamental right to the protection of personal data might result in higher awards than were previously the case.[69]

3. REGULATORY ENFORCEMENT

48– 014 General processing

In relation to general processing,[70] the Information Commissioner (as the 'supervisory authority' for the purposes of the GDPR) is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data.[71] As such, the Commissioner can instigate regulatory processes without having received a complaint. On the other hand, where a data subject (or a body or organisation representative of one or more data subjects) lodges a complaint with the Information Commissioner in relation to general processing, the Commissioner must investigate it to the extent appropriate and must inform the data subject (or representative body) of the progress and outcome of the investigation within a reasonable period.[72] Unless manifestly unfounded or excessive, the Information Commissioner may not impose a charge on a data subject for dealing with such complaints.[73] As part of its regulatory powers in relation to general processing, the Information Commissioner may:

(a) Order the controller and the processor and, where applicable, the controller or

---

67 DPA 2018 ss 58(2) and 61 in relation to law enforcement processing, s 104(2) in relation to intelligence services processing.

68 DPA 2018 s 169(4). The 'data protection legislation' means the GDPR, the applied GDPR, the DPA 2018 and regulations thereunder, and regulations made under the European Communities Act 1972 s 2(2) that related to the GDPR or the LED: DPA 2018 s 3(9).

69 As to damages under the DPA 2018, see §49– 008. In relation to the recognition of the fundamental right to the protection of personal data, see §§7– 019 to 7– 023. Initially, a superannuated approach to compensation had been taken under the DPA 1998, exemplified by Buxton LJ in *Johnson v Medical Defence Union* [2007] EWCA Civ 262, [2007] 3 CMLR 9, (2007) 96 BMLR 99 stating:

> There is no compelling reason to think that 'damage' in the directive has to go beyond its root meaning of pecuniary loss. Nor do I accept Mr Howe's contention that the fact that the directive envisages the protection of rights under art 8 of the European Convention (as to which, see [15] above) entails that compensation must be available in every case for loss of a type or category that would be covered by art 8: for example, damages for distress (at [74]).

Arden LJ dissented. In rejecting this passage as good law, the Court of Appeal in *Vidal Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003 was compelled to treat it as obiter (at [61]-[69]).

70 On the division between 'GDPR processing', 'applied GDPR processing', 'law enforcement processing' and 'intelligence services processing' see §§8– 002 and 9– 002.

71 GDPR Arts 51(1) and 57(1)(a) (in relation to GDPR processing) and DPA 2018 Sch 6 para 40(a)(i) in relation to applied GDPR processing; DPA 2018 s 115(1) in relation to both GDPR processing and applied GDPR processing. As to those fundamental rights and freedoms, see §8– 006.

72 GDPR Art 57(1)(f) (in relation to GDPR processing) and DPA 2018 Sch 6 para 46 (in relation to applied GDPR processing); DPA 2018 s 165(1) in relation to both GDPR processing and applied GDPR processing. A data subject has a right to lodge a complaint with the Information Commissioner: GDPR Art 77 (in relation to GDPR processing) and DPA 2018 Sch 6 para 50 (in relation to applied GDPR processing). The Information Commissioner is required to facilitate the submission of complaints: GDPR Art 57(2).

73 GDPR Art 57(3)-(4) (in relation to GDPR processing) and DPA 2018 Sch 6 para 46 (in relation to applied GDPR processing). Instead of charging a reasonable fee for a manifestly unfounded or excessive request, the Information Commissioner may refuse to act on the request: GDPR Art 57(4).