Neutral Citation Number: [2018] EWCA Civ 2339

Case No: A2/2018/0090

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
THE HON. MR JUSTICE LANGSTAFF
[2017] EWHC 3113 (QB)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 22/10/2018

Before:

THE MASTER OF THE ROLLS
LORD JUSTICE BEAN
and
LORD JUSTICE FLAUX

- -

Between:

	WM MORRISON SUPERMARKETS PLC	**Appellant**
	- and -	
	VARIOUS CLAIMANTS	**Respondent**

- -
- -

Anya Proops QC and Rupert Paines (instructed by **DWF LLP**) for the **Appellant**
Jonathan Barnes and Victoria Jolliffe (instructed by **JMW Solicitors LLP**) for the **Respondents**

Hearing dates: 9 and 10 October 2018

- -

Judgment Approved

Sir Terence Etherton MR, Lord Justice Bean and Lord Justice Flaux:

Introduction

1. The central issue on this appeal is whether, on the facts, an employer is liable in damages to those of its current or former employees whose personal and confidential information has been misused by being disclosed on the web by the criminal act of another employee, who had a grudge against the employer, in breach of the Data Protection Act 1998 ("the DPA") and in breach of that employee's obligation of confidence.

2. It is an appeal from the order of Langstaff J dated 1 November 2017 by which he ordered that the appellant, Wm Morrison Supermarkets plc ("Morrisons"), which is the defendant in the proceedings, is liable in damages to the claimants, who are over 5,000 employees or former employees of Morrisons, for the acts of disclosure of their personal information by a former employee, Andrew Skelton.

3. The appeal concerns whether the Judge was correct to hold that Morrisons is vicariously liable to the claimants for the actions of Mr Skelton.

4. The Judge himself gave permission to appeal.

Background

5. It is necessary to describe the factual background in some detail as vicarious liability is highly fact specific. The following, which we gratefully take from the judgment of the Judge, is not as full as the Judge's account but is sufficient for the purposes of the appeal.

6. At the relevant time Mr Skelton was a senior IT internal auditor employed by Morrisons. Following a disciplinary hearing for an incident involving his unauthorised use of Morrisons' postal facilities for his private purposes, he was given a formal verbal warning on 18 July 2013. Mr Skelton was annoyed by the disciplinary proceedings and the sanction. They left him with a grudge against Morrisons.

7. On 1 November 2013 KPMG, Morrisons' external auditor, requested a number of categories of data from Morrisons in order to undertake the annual audit. That request included a copy of Morrisons' payroll data. Michael Leighton, of the HR department, copied the data onto an encrypted USB stick. He took the USB stick personally to Mr Skelton, who downloaded the data from the stick onto his laptop computer, which was itself encrypted. Mr Skelton subsequently copied the data onto another encrypted USB stick, which had been supplied by KPMG, and which he returned to KPMG.

8. On 18 November Mr Skelton, when at work, copied the payroll data onto a personal USB with a view to the later commission of the crime consisting of disclosure of the data.

9. On 12 January 2014, using the payroll data that he had copied onto his personal USB, Mr Skelton posted a file containing the personal details of 99,998 employees of Morrisons on a file sharing website. He used the initials and date of birth of another employee in a deliberate attempt to frame him. Shortly afterwards, links to the website were also placed elsewhere on the web. The data consisted of the names, addresses, gender, dates of birth, phone numbers (home or mobile), national insurance numbers, bank sort codes, bank account numbers and the salary which the employee in question was being paid.

10. On 13 March 2014 Mr Skelton, acting anonymously, sent a CD containing a copy of the data to three newspapers in the UK, one of which was the Bradford Telegraph and Argus, a newspaper local to Bradford where Morrisons has its head office. The anonymous sender purported to be a concerned person who had worryingly discovered that payroll data relating to almost 100,000 Morrisons' employees was available on the web. The covering letter with the CD gave a link to the file-sharing site.

11. The information was not published by any of the newspapers concerned. The Bradford Telegraph and Argus told Morrisons of it. Morrisons was about to announce its annual

financial reports. The revelation of the data leak had serious implications for the share value of Morrisons. There was also an immediate concern that the information might be used by outsiders to access the bank accounts of individual employees or used to aid identity theft.

12. Morrisons' head management was alerted to the disclosure on 13 March 2014. Within a few hours they had taken steps to ensure that the website had been taken down. Morrisons also alerted the police.

13. Mr Skelton was arrested on 19 March 2014. He was charged with fraud, an offence under the Computer Misuse Act 1990 and under section 55 of the DPA. He was tried at Bradford Crown Court in July 2015, and was convicted. He was sentenced to a term of eight years imprisonment.

The DPA

14. The DPA was enacted pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Directive"). Provisions in the Directive to which we were referred in the course of oral submissions are set out in Appendix 1 to this judgment.

15. Relevant provisions of the DPA are set out in Appendix 2 to this judgment.

The proceedings

16. Following a Group Litigation Order made by Senior Master Fontaine on 24 November 2015, these proceedings were commenced by 5,518 employees of Morisons on 8 December 2015 when a claim form was issued for damages and interest for misuse of private information, breach of confidence and breach of statutory duty owed under section 4(4) of the DPA. The claim form was accompanied by Particulars of Claim. The claimants claimed that Morrisons is primarily liable under those heads of claim but, if not, then Morrisons is liable vicariously for the wrongful conduct of Mr Skelton.

17. Morrisons served a Defence dated 3 February 2016 denying all liability.

18. Following directions for a split trial on liability and damages, the trial as to liability took place before the Judge between 9 and 19 October 2017.

The judgment

19. The Judge handed down a careful, comprehensive and lengthy written judgment on 1 December 2017. The following is a brief summary sufficient to provide a context for the present appeal.

20. The Judge held (at [51] and [65]) that Morrisons was not the data controller at the time of any breach of Data Protection Principles ("DPP") 1, 2, 3 and 5 in respect of the information later disclosed on the web, and accordingly Morrisons owed no duty to the claimants under the DPA in respect of which it was in breach, unless it were the duty to comply with DPP 7. Mr Skelton was the data controller in respect of that information.

21. The Judge further held (at [66]) that Morrisons was not directly liable in respect of any breach of confidence or misuse of private information since it was not Morrisons which disclosed the information or misused it. It was Mr Skelton, acting without authority and criminally.

22. The Judge identified (at [74]) the following six respects in which it was alleged that Morrisons fell short of its obligations under DPP 7 while it was the data controller: failing to manage/mentor Mr Skelton to prevent a grudge developing; failing to monitor Mr Skelton's IT usage so as to identify that Mr Leighton's initial attempt to send the data to Mr Skelton's computer had bounced back (having been intercepted by Morrisons' "quarantine" area, designed to divert for further attention emails that for some reason may be suspicious); failing to identify that Mr Skelton was researching the "TOR" (acronym for "The Onion Router") network (for software which is capable of disguising the individual identity of a computer which has accessed the internet); failing to deny Mr Skelton access to the data; providing the data to Mr Skelton via a USB stick which was not encrypted; and failing to ensure that Mr Skelton deleted the data from his computer by about 21 November 2013.

23. The Judge held that, save in relation to the last item -- data deletion -- Morrisons had provided adequate and appropriate controls in relation to each of those matters. The Judge made the following particular findings, among others, on those particular matters. He said (at [95]) that the incident for which Mr Skelton was disciplined did not itself suggest that Mr Skelton was not to be trusted. The Judge found (at [96]) that the technological and organisational measures current in 2013 and 2014 at their best could not altogether prevent the risk posed by a rogue employee who was trusted and had given no reason to doubt his trustworthiness. The Judge said (at [97]) that no one in employment at Morrisons knew, nor ought they to have known, that Mr Skelton bore a grudge against Morrisons, and was not to be trusted with data. The Judge found (at [97]) that, even if a senior manager had been aware that the email sent by Mr Leighton to Mr Skelton, attaching the payroll data, had bounced back, it would not have alerted Morrisons to the risk which Mr Skelton posed to the data.

24. The Judge dismissed (at [99]-[110]) the allegation that Morrisons should have been aware that Mr Skelton was attempting to research the TOR network on the grounds that it was not feasible, sensible or practicable for Morrisons to have implemented a system that could proactively have detected that Mr Skelton was researching the TOR network when he did, and, moreover, any such system would probably have amounted to an unlawful interference with employees' rights to privacy and family life. The Judge added (at [110]) that, even if there had been a failure to monitor employees' internet search usage, it is unlikely that it would have prevented the data disclosure by Mr Skelton. The Judge found (at [111]) that the USB stick used to convey the payroll data to Mr Skelton was encrypted and its use was not a breach of DPP 7, nor did the use of it cause or contribute to the disclosure which later occurred.

25. So far as concerns data deletion, the Judge found (at [118]) that there was no organised system for the deletion of data such as the payroll data stored for a brief while on Mr Skelton's computer. To the extent that there was no failsafe system in respect of it, the Judge concluded that Morrisons fell short of the requirements of DPP 7. He said that, where data is held outside the usual secure repository used for it, there is an unnecessary risk of proliferation and of inadvertent disclosure (let alone deliberate action by an employee) revealing some of that data. Morrisons took that risk and did not need to do so. Organisational measures which would have been neither too difficult nor too onerous to implement could have been adopted to minimise it. The Judge also found (at [121]), however, that in the particular circumstances of the present case, by the time it would have been appropriate to conduct any check on deletion, the probability was that the information had already been copied by Mr Skelton; and, accordingly, to the extent that Morrisons fell short of DPP 7 in its duty to take appropriate organisational measures to guard against unlawful disclosure and data loss, that failure neither caused nor contributed to the disclosure which occurred.

26. As Morrisons did not directly misuse or authorise or carelessly permit the misuse of any information personal to the employees, the Judge dismissed (at [124]-[126]) the claims against Morrisons in equity and at common law for primary liability for breach of confidence and misuse of personal information.

27. The Judge then addressed the issue of Morrisons' vicarious liability. He rejected what he described as two preliminary points on vicarious liability advanced by Morrisons. The first was whether the DPA by its terms excludes any possibility of vicarious liability. The second was whether the effect of the DPA was to exclude any scope for vicarious liability under the common law tort of misuse of private information or the equitable action for breach of confidence.

28. The Judge, having cited *Harrison v National Coal Board* [1951] AC 639, *Rottman v Commissioner of Police of the Metropolis* [2002] UKHL 20, [2002] 2 AC 692, *Re McKerr* [2004] UKHL 12, [2004] 1 WLR 807*, Majrowski v Guy's and St Thomas' NHS Trust* [2005] EWCA Civ 251, [2005] QB 848, *R (Child Poverty Action Group) v Secretary of State for Work and Pensions* [2010] UKSC 54, [2011] 2 AC 15, *Mohamud v William Morrison Supermarkets plc* [2016] UKSC 11; [2016] AC 677, *Bellman v Northampton Recruitment Ltd* [2016] EWHC 3104, QB; [2017] ICR 543, and *Various Claimants v Barclays Bank plc* [2017] EWHC 1929 (QB) 126; [2017] IRLR 1103, rejected both points.

29. On the first point, he said (at [156]) that, merely because the DPA had the effect that Mr Skelton became data controller of the information did not exclude vicarious liability for his breaches of statutory duty under the DPA in respect of that information. He accepted the argument for the claimants that the DPA was intended to supplement, not exclude, what would otherwise be liability.

30. As to the second point, he said (at [160]) that the purpose of the Directive was to provide greater protection for the rights of data subjects and that it is generally open to a member state to augment a minimum EU-wide standard of protection where protection is the aim. Accordingly, he could not conclude that the DPA excludes common law and equitable actions in respect of the same data disclosure. He said (at [162]) that the tort of misuse of

private information and the action for breach of confidence do not run counter to the tenor of the DPA and are not incompatible with the statutory scheme: they are complementary.

31. Turning to the principles of vicarious liability, the Judge referred to a large number of further authorities: *Armes v Nottinghamshire County Council* [2017] UKSC 60; [2018] AC 355, *Bazley v Curry* (1999) 174 DLR (4th) 45*, Lister v Hesley Hall Ltd* [2002] A.C. 215, *Rose v Plenty* [1976] 1 WLR 141*, Century Insurance Co Ltd v Northern Ireland Road Transport Board* [1942] AC 509, *Mattis v Pollock* [2003] EWCA Civ 887, *Williams v Hemphill* [1966] UKHL 3, *Credit Lyonnais v Export Credits Guarantee Department [*2000] AC 486, *Deatons v Flew* [1949] 79 CLR 370 (High Court of Australia), *Irving v Post Office* [1987] IRLR 289, *Weddall v Barchester Healthcare* [2012] EWCA Civ 25, *Bernard v Attorney General of Jamaica* [2004] UKPC 47, *Brown v Robinson* [2004] UKPC 56, *Fennelly v Connex Southeastern Limited* [2000] EWCA Civ 5568; [2001] IRLR 390, *Axon v Ministry of Defence* [2016] EWHC 787 (QB*)*; [2016] EMLR 20*, Zuijs v. Wirth Brothers Proprietary, Ltd* (1955) 93 C.L.R. 561, 571, *Ready-Mixed Concrete v Minister of Pensions and National Insurance* [1968] 2 QB 497), and *Various Claimants v Catholic Child Welfare Society and others* [2012] UKSC 56, [2013] 2 A.C. 1. The Judge held (at [197) that, adopting the broad and evaluative approach encouraged by Lord Toulson in *Mohamud*, there was a sufficient connection between the position in which Mr Skelton was employed and his wrongful conduct, put into the position of handling and disclosing the data as he was by Morrisons, to make it right for Morrisons to be held vicariously liable, whether for breach of duty under the DPA, a misuse of private information, or a breach of the duty of confidence. The findings of fact which led him to that conclusion are set out in [184] of the judgment, which we quote at [73] below.

32. The Judge concluded his judgment by saying that the point which most troubled him in reaching his conclusions was the submission that the wrongful acts of Mr Skelton were deliberately aimed at the party whom the claimants sought to hold responsible, such that to reach the conclusion he had might seem to render the court an accessory in furthering Mr Skelton's criminal aims. It would appear that it was for that reason that he gave permission to appeal.

Grounds of appeal

33. There are three grounds of appeal. First, the Judge ought to have concluded that, on its proper interpretation and having regard to the nature and purposes of the statutory scheme, the DPA excludes the application of vicarious liability. Second, the Judge ought to have concluded that, on its proper interpretation, the DPA excludes the application of causes of action for misuse of private information and breach of confidence and/or the imposition of vicarious liability for breaches of the same. Third, the Judge was wrong to conclude (a) that the wrongful acts of Mr Skelton occurred during the course of his employment by Morrisons, and, accordingly, (b) that Morrisons was vicariously liable for those wrongful acts.

Respondent's notice

34. The claimants have issued a respondent's notice seeking to uphold the order of the Judge

on the additional ground that, in evaluating whether there was a sufficient connection between Mr Skelton's employment and his wrongful conduct to make it right for Morrisons to be held vicariously liable, the Judge ought to have taken into account that Mr Skelton's job included the task or duty delegated to him by Morrisons of preserving confidentiality in the claimants' payroll information.

35. It is important to observe that the claimants do not challenge on the appeal the Judge's dismissal of the claims against Morrisons for breach of its statutory duties under the DPA; and neither side challenges the Judge's finding that Mr Skelton, and not Morrisons, was the data controller under the DPA in respect of the data wrongfully copied by Mr Skelton onto his personal USB stick and subsequently disclosed by him on the internet (as to which, see *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd* [2017] EWCA Civ 121, [2018] QB 256 at [70]-[71]).

Discussion

The first and second grounds of appeal

36. It is convenient to consider the first and second grounds of appeal together because, in substance, the first ground of appeal is merely a stepping stone for Morrisons' contention that, in relation to the processing of personal data within the ambit of the DPA, it is a necessary implication of the DPA that there can be no vicarious liability for the common law tort of misuse of private information or for breach of the equitable duty of confidence.

37. There is no pleaded claim against Morrisons on the ground of vicarious liability for the statutory tort of breach of the DPA by Mr Skelton. The pleaded claim against Morrisons under the DPA is in respect of its primary liability for breach of its own direct statutory obligations imposed by the DPA. In the prayer to the Particulars of Claim damages are claimed pursuant to section 13 of the DPA for breach of Morrisons' own statutory duties. The other two heads of claim in the prayer to the Particulars of Claim are for damages for misuse of private information and damages for breach of confidence. Morrisons' vicarious liability arises, if at all, under those causes of action in respect of Mr Skelton's wrongful acts.

38. The Judge, in accepting the claimants' argument that an employer can be vicariously liable for the statutory tort of an employee data controller in breach of the DPA, did not refer to that pleading point. It does not matter, however, because, as we have said, from Morrisons' perspective the issue is simply a plank in its argument that the DPA provides a comprehensive statutory code for the wrongful processing of personal data, and it expressly or impliedly excludes any scope for liability on an employer for the wrongful processing of personal data by an employee, whether the data controller is the employer or the employee.

39. Ms Anya Proops QC, for Morrisons, made extensive and elaborate submissions on the first and second grounds of appeal but the essence of her argument may be simply stated as follows.

40. The common law principle of vicarious liability is not confined to common law wrongs. It holds good for a wrong comprising a breach of statutory duty provided the statute does not expressly or impliedly indicate otherwise: *Majrowski v Guy's and St Thomas's NHS Trust* [2006] UKHL 34, [2007] 1 AC 224 at [10] Lord Nicholls). The DPA does indicate the contrary. Pursuant to the Directive, the DPA seeks to achieve a balance between the right to privacy and the free flow of personal data from one member state to another in the interests of economic and social progress. It imposes express obligations on the data controller, primarily the obligation under section 4(4) to comply with the DPP. In accordance with ordinary principles of EU jurisprudence, those obligations are to be interpreted as proportionate ones. They are in any event expressly qualified in important respects by reference to what is appropriate or reasonable. So, DPP 7 requires that "appropriate" technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

41. What is "appropriate" is related to the state of technological development and the cost of implementing any measures as well as the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage, and the nature of the data to be protected: Schedule 1 Part II para. 9. Importantly, under DPP 7 the data controller must take "reasonable steps" to ensure the reliability of any employees of his who have access to the personal data: Schedule 1 Part II para. 10. The DPA, therefore, expressly recognises the potential liability of a data controller for the wrongful processing of data by his employees. Instead, however, of imposing a vicarious liability, which is a strict liability irrespective of the employer's fault, it imposes a primary liability on the employer restricted to taking "reasonable steps" to ensure the reliability of the relevant employees. Further, section 13(3) provides that it is a defence to an action by an individual for compensation from the data controller for breach of any of the requirements of the DPA that the data controller has taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. In effect, so far as concerns civil liability, the liability is based on fault or culpability: cf. criminal liability under section 55 of the DPA.

42. Ms Proops also submitted that there are public policy considerations supporting an interpretation of the DPA which avoids imposing a disproportionate burden on the employer, particularly bearing in mind the difficulty of securing something intangible like data, the potential cost of ensuring compliance and the potential exposure of even small entities to claims for compensation for distress (as recognised in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003) by large numbers of victims (as in the present case), all of which might have a chilling effect on enterprise and efficiency. The DPA imposes no express liability whatsoever on an employer, who is not a data controller, for wrongful processing of data in breach of the DPA by an employee who is a data controller and so subject to all the obligations and liabilities of a data controller under the DPA. For all these reasons, on the proper interpretation of the DPA, there is no scope for the subsistence of vicarious liability under the common law on an employer for breach of the statutory duty of an employee data controller to comply with the DPA.

43. So far as concerns liability at common law for misuse of private information or in equity for breach of confidence, Ms Proops' core submission was that the DPA is specialist legislation which was intended by Parliament to cover the entire field of liability of an employer for the wrongful processing of personal data by an employee. In that connection she emphasised that the DPA, the tort of misuse of private information and

the cause of action in equity for breach of confidence all relate to the same subject matter – privacy. She also relied on both the decision of the Court of Justice of the European Union ("the CJEU") in C-101/01 *Criminal proceedings against Lindqvist* [2004] QB 1014 and the judgment of Lord Dyson JSC in *R (Child Poverty Action Group) v Secretary of State for Work and Pensions* [2010] UKSC 54, [2011] 2 AC 15.

44. One of the questions referred to the CJEU in *Lindqvist* was whether it is permissible for member states to provide for greater protection for personal data or a wider scope than are required under the Directive. The CJEU's reply was that member states could only do so in respect of areas not included within the scope of the Directive. The CJEU said as follows:

> "96 The harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is on that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate.
>
> 97 It is true that Directive 95/46 allows the member states a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations, as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life.
>
> 98 On the other hand, nothing prevents a member state from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it.
>
> 99 In the light of those considerations, the answer to the seventh question must be that measures taken by the member states to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a member state from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof, provided that no other provision of Community law precludes it."

45. In the *Child Poverty Action Group* case the issue was whether the right to recover overpaid Social Security benefits made pursuant to an erroneous award was restricted to the right conferred by section 71 of the Social Security Administration Act 1992, which applied only where there has been overpayment as a consequence of either misrepresentation or non-disclosure, or whether there could be recovery by way of a claim in restitution at common law for money paid by mistake of law or fact. The Supreme Court held that the Secretary of State could only reclaim overpayments of

benefits made pursuant to incorrect awards under section 71 of the 1992 Act; that is to say that section 71 constituted a comprehensive and exclusive scheme for dealing with all overpayments of benefit made pursuant to awards. Ms Proops relied on the judgment of Lord Dyson, in which he said in obiter remarks, that the test is whether in all the circumstances Parliament must have intended a common law remedy to coexist with the statutory remedy.

46. He elaborated as follows.

> "33 If the two remedies cover precisely the same ground and are inconsistent with each other, then the common law remedy will almost certainly have been excluded by necessary implication. To do otherwise would circumvent the intention of Parliament. A good example of this is *Marcic*, where a sewerage undertaker was subject to an elaborate scheme of statutory regulation which included an independent regulator with powers of enforcement whose decisions were subject to judicial review. The statutory scheme provided a procedure for making complaints to the regulator. The House of Lords held that a cause of action in nuisance would be inconsistent with the statutory scheme. It would run counter to the intention of Parliament.
>
> 34 The question is not whether there are *any* differences between the common law remedy and the statutory scheme. There may well be differences. The question is whether the differences are so substantial that they demonstrate that Parliament could not have intended the common law remedy to survive the introduction of the statutory scheme. The court should not be too ready to find that a common law remedy has been displaced by a statutory one, not least because it is always open to Parliament to make the position clear by stating explicitly whether the statute is intended to be exhaustive. The mere fact that there are some differences between the common law and the statutory positions is unlikely to be sufficient unless they are substantial. The fact that the House of Lords was divided in *Total Network SL* [2008] AC 1174 shows how difficult it may sometimes be to decide on which side of the line a case falls. The question is whether, looked at as a whole, a common law remedy would be incompatible with the statutory scheme and therefore could not have been intended by coexist with it.

47. Ms Proops submitted that it is clear that there are highly significant inconsistencies between the liabilities under the DPA of employers, whether they or their employees are data controllers, and the strict liability imposed at common law on principals by way of vicarious liability for the defaults of employees and others. As stated earlier, the requirements imposed on an employer under DPP 7 are qualified by concepts of appropriateness and reasonableness, and liability for compensation for contravention by a data controller of the requirements of the DPA is limited to cases where the data controller has failed to take reasonable care to comply with the requirement concerned. As also stated earlier, Morrisons contend that the terms of the DPA expressly or impliedly exclude the continued imposition of vicarious liability under the common law on an employer for breach of the statutory duty of an employee data controller to comply

with the DPA.

48. That analysis was ably advanced by Ms Proops. We consider it is clear, however, that whatever the position on the first ground of appeal, the vicarious liability of an employer for misuse of private information by an employee and for breach of confidence by an employee has not been excluded by the DPA.

49. The applicable principle for determining that issue is clear. The question is whether, on the proper interpretation of the DPA, it is implicit that Parliament intended to exclude such vicarious liability. In her skeleton argument, Ms Proops criticised the Judge's test of "necessary implication" but we consider that test to be entirely appropriate. If the statutory code covers precisely the same ground as vicarious liability at common law, and the two are inconsistent with each other in one or more substantial respects, then the common law remedy will almost certainly have been excluded by necessary implication. As Lord Dyson said in the *Child Poverty Action Group* case (at [34]) the question is whether, looked at as a whole, the common law remedy would be incompatible with the statutory scheme and therefore could not have been intended to coexist with it.

50. There are three major obstacles to Morrisons' proposition in the present case that the DPA has by necessary implication excluded an employer's vicarious liability at common law for an employee's misuse of private information and breach of confidence.

51. The first, which is an obvious point, is that, if Parliament had intended such a substantial eradication of common law and equitable rights, it might have been expected to say so expressly. So far as concerns misuse of private information, Ms Proops submitted that the common law tort of misuse of private information was only established by *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457, long after the DPA and, even more so, its statutory predecessor the Data Protection Act 1984. We doubt that is a correct analysis since, as Lord Nicholls observed in *Campbell* (at [14]), the courts had recognised long before the DPA that, irrespective of any confidential relationship, the law imposes a duty of confidence whenever a person receives information he or she knows or ought to know is fairly and reasonably to be regarded as confidential. The nomenclature "misuse of private information" may only have been coined in *Campbell* but the existence of the cause of action was known to exist well before the DPA.

52. Furthermore, as Mr Jonathan Barnes, counsel for the claimants, observed, the "processing" of data is defined so widely in section 1(1) of the DPA, that it is capable of embracing matters as varied as breach of copyright, defamation, harassment and negligence. If Parliament had intended to exclude the common law vicarious liability of an employer for the processing of information amounting to such a wide variety of non-statutory wrongs by an employee, who happened to be the data controller under the DPA, it is surprising that Parliament did not say so expressly.

53. Secondly, despite the wording of the second ground of appeal ("the DPA excludes the application of these judge-made causes of action and/or the imposition of vicarious liability for breaches of the same") and some suggestions in Ms Proops' opening oral submissions that the DPA impliedly excluded the entire tort of misuse of private information and the cause of action for breach of confidence in relation to the processing of personal data within the ambit of the DPA, she made it clear in her further oral

submissions that only vicarious liability at common law and in equity was excluded. That is, of course, a necessary facet of the claimants' position that Mr Skelton was not only in breach of the primary obligations laid on him by the DPA as data controller of the information disclosed by him but he was also primarily liable for the tort of misuse of private information and for breach of confidence in equity.

54. This is nevertheless an important concession. It is clear from the passages in the judgment of the CJEU quoted above that the Directive was intended to effect a complete harmonisation of the law affecting member states in order to achieve a balance between the free movement of personal data and the protection of private life, subject only to the right of member states to provide a different legal regime in national legislation for areas not included in the scope of the Directive and not otherwise contrary to EU law. There would therefore be some logic in an argument that, interpreted against that background, the DPA was intended to cover the entire field relating to the processing of data within the ambit of the DPA, to the exclusion of common law and equitable remedies. That would eliminate the possible difficulty of discrepancies between liability at common law or in equity, on the one hand, and liability under the DPA, on the other hand, due, for example, to the exemptions in Part IV of the DPA and the limitation of liability for compensation under section 13 of the DPA.

55. It is true that in *Campbell*, the courts at all stages – first instance, Court of Appeal and House of Lords – assumed that the cause of action for breach of confidence and (as characterised in the House of Lords) for misuse of private information – subsist alongside the DPA. Ms Proops observed that the contrary was not argued in that case. She has not, however, sought to argue the contrary before us.

56. Morrisons' acceptance that the causes of action at common law and in equity operate in parallel with the DPA in respect of the primary liability of the wrongdoer for the wrongful processing of personal data while at the same time contending that vicarious liability for the same causes of action has been excluded by the DPA is, on the face of it, a difficult line to tread. That is not least because it may be said to present an inconsistency in the application of one of the principal objects of the Directive and of the DPA, namely the protection of privacy and the provision of an effective remedy for its infringement (including by an employee of limited means), rather than their curtailment.

57. Thirdly, the difficulty of treading that line becomes insuperable on the facts of the present case because, as was emphasised by Mr Barnes, the DPA says nothing at all about the liability of an employer, who is not a data controller, for breaches of the DPA by an employee who is a data controller. That is the situation here in respect of the payroll data disclosed by Mr Skelton. It is common ground on this appeal that he, and not Morrisons, was the data controller under the DPA in respect of that data. As Ms Proops herself repeatedly emphasised in her submissions, in terms of processing duties and liability, the DPA is only concerned with the primary liability and obligations of the data controller. It has nothing at all to say about the liability of someone else for wrongful processing by the data controller. Parliament has not entered that field at all.

58. That is quite different from the situation in the cases on which Ms Proops relied. In those cases the legislation expressly and specifically addressed the circumstances which, it was contended, also gave rise to a common law remedy, but there were substantial

differences between the two of them. The court held, as a matter of statutory interpretation, that the statutory remedy was exclusive: see the *Child Poverty Action Group* case (the facts of which, and the decision on section 71 of the Social Security Administration Act 1992, are summarised above); *R (Omar) v Secretary of State for Foreign and Commonwealth Affairs* [2013] EWCA Civ 118, [2014] QB 112 (held: the regime set out in the Crime (International Co-operation) Act 2003 for the obtaining of evidence for use in foreign proceedings was an exclusive procedure, which precluded a remedy under the principles in *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133); *Investment Trust Companies v Revenue and Customs Commissioners* [2017] UKSC 29, [2018] AC 275 (held: sections 80 and 80A of the Value Added Tax Act 1994 and the Value Added Tax Regulations 1995 provided an exhaustive code for the repayment by the commissioners of overpaid VAT and excluded non-statutory claims by anyone against the commissioners for overpaid VAT, such as the common law cause of action for unjust enrichment).

59. Further, on the issue of inconsistency, the contrast between the fault based primary liability on an employer data controller under the DPA and the imposition of a strict vicarious liability on an employer for the defaults of an employee data controller is in truth no more of an anomaly than the position at common law. The common law imposes the same strict liability on an employer who is guilty of no fault. The legal policy which limits the imposition of that strict liability is the requirement of a sufficient connection between the default of the employee and the running of the employer's enterprise.

60. In conclusion, the concession that the causes of action for misuse of private information and breach of confidentiality are not excluded by the DPA in respect of the wrongful processing of data within the ambit of the DPA, and the complete absence of any provision of the DPA addressing the situation of an employer where an employee data controller breaches the requirements of the DPA, lead inevitably to the conclusion that the Judge was correct to hold that the common law remedy of vicarious liability of the employer in such circumstances (if the common law requirements are otherwise satisfied) was not expressly or impliedly excluded by the DPA.

The third ground of appeal

61. The submissions of Ms Proops in relation to the principles at common law for vicarious liability focused on the tests set out in the most recent decision of the Supreme Court on this issue, *Mohamud v Wm Morrison Supermarkets plc* [2016] AC 667. In that case, a petrol pump attendant (Mr Khan) assaulted a customer. Lord Toulson JSC, with whom all the other Justices agreed (though Lord Dyson MR gave a separate judgment) said at [40] that:-

> "The risk of an employee misusing his position is one of life's unavoidable facts."

62. He continued at [44]-[46] and [48]:-

> "44. In the simplest terms, the court has to consider two matters. The first question is what functions or "field of activities" have been entrusted by the employer to the employee, or, in everyday

language, what was the nature of his job. As has been emphasised in several cases, this question must be addressed broadly……..

45. Secondly, the court must decide whether there was sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable under the principle of social justice which goes back to Holt CJ. To try to measure the closeness of connection, as it were, on a scale of 1 to 10, would be a forlorn exercise and, what is more, it would miss the point. The cases in which the necessary connection has been found for Holt CJ's principle to be applied are cases in which the employee used or misused the position entrusted to him in a way which injured the third party. *Lloyd v Grace, Smith & Co*, *Pettersson v Royal Oak Hotel Ltd* and *Lister v Hesley Hall Ltd* were all cases in which the employee misused his position in a way which injured the claimant, and that is the reason why it was just that the employer who selected him and put him in that position should be held responsible. By contrast, in *Warren v Henlys Ltd* any misbehaviour by the petrol pump attendant, qua petrol pump attendant, was past history by the time that he assaulted the claimant. The claimant had in the meantime left the scene, and the context in which the assault occurred was that he had returned with the police officer to pursue a complaint against the attendant.

46. Contrary to the primary submission advanced on the claimant's behalf, I am not persuaded that there is anything wrong with the *Lister* approach as such. It has been affirmed many times and I do not see that the law would now be improved by a change of vocabulary. Indeed, the more the argument developed, the less clear it became whether the claimant was advocating a different approach as a matter of substance and, if so, what the difference of substance was.

…

48. Mr Khan's motive is irrelevant. It looks obvious that he was motivated by personal racism rather than a desire to benefit his employer's business, but that is neither here nor there."

63. The first question posed by Lord Toulson was answered in the present case by the Judge in his findings at [185]-[186] of his judgment in terms which we regard as plainly correct:-

"185. …….I find that Morrisons deliberately entrusted Skelton with the payroll data. It was not merely something to which work gave him access: dealing with the data was a task specifically assigned to him. Associated with this, I find that in his role with Morrisons, day in and day out, he was in receipt of information which was confidential or to have limited circulation only: and he was appointed on the basis that this would happen, and he could be trusted to deal with it safely. Morrisons took the risk they

might be wrong in placing the trust in him.

> 186. …..[H]is role in respect of the payroll data was to receive and store it, and to disclose it to a third party. That in essence was his task, so far as the payroll data went: the fact that he chose to disclose it to others than KPMG was not authorised, but it was nonetheless closely related to what he was tasked to do."

64. In relation to Lord Toulson's second question (which is at the heart of the argument in the present case), Ms Proops submitted that the close connection test is not satisfied, since the tortious act which caused the harm was done by Mr Skelton at his home, using his own computer, on a Sunday, several weeks after he had downloaded the data at work onto his personal USB stick.

65. The first aspect of this submission is the argument that the online disclosure of the data in January 2014 was the act which caused the harm; and that even if, contrary to Morrisons' submissions, the original copying in November 2013 was done in the course of employment, the disclosure was not. Ms Proops relied on *Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Department* [2000] 1 AC 486 for the proposition that every necessary element of the tort which founds liability must occur within the course of employment if vicarious liability is to apply. Lord Woolf MR said at page 495:-

> "[the] conduct for which the servant is responsible must constitute an actionable tort and to make the employer responsible for that tort the conduct necessary to establish the employee's liability must have occurred within the course of employment. … Before these can be vicarious liability, all the features of the wrong which are necessary to make the employee liable have to have occurred in the course of the employment."

66. In the present case the claimants' causes of action in tort against Mr Skelton were already established when he improperly downloaded their data onto his USB stick. At that stage, had any of them been aware of what happened, they could as a matter of law have claimed at least nominal damages and sought an injunction to prevent dissemination of the data. We agree with the Judge that the issue in the *Credit Lyonnais* case was not whether the acts complained of fell within the course of employment but rather (as he said at [189]):-

> "whether acts which were committed without the course of employment, which were not in themselves tortious, could be aggregated with acts of another party so as to render the employee a joint tortfeasor with that party, for whose joint acts the employer would be held vicariously liable."

67. A case on very different facts on which Ms Proops strongly relied was *Warren v Henlys* [1948] 2 All ER 945: like *Mohamud,* a case of an assault by a petrol pump attendant on a customer. The reported judgment was only a ruling by a trial judge (Hilbery J) but since it was cited with approval by Lord Toulson in *Mohamud* its status has been somewhat enhanced. Ms Proops relies on the observation about *Warren* by Lord Toulson at [45] of

Mohamud that "any misbehaviour by the petrol pump attendant *qua* petrol pump attendant was past history by the time he assaulted the Claimant"; and argues that what Mr Skelton had done at work in November was past history by the time he distributed the data from home in January.

68. In this context, it is important to look closely at the precise facts of *Warren v Henlys*. These were summarised by Lord Toulson at [31]-[32] as follows:-

> "31. In *Warren v Henlys Ltd* [1948] 2 All ER 935 a customer at a petrol station had an angry confrontation with the petrol station attendant, who wrongly suspected him of trying to make off without payment. The customer became enraged at the manner in which he was spoken to by the attendant. After paying for the petrol, the customer saw a passing police car and drove off after it. He complained to the police officer about the attendant's conduct and persuaded the officer to return with him to the petrol station. The officer listened to both men and indicated that he did not think that it was a police matter, whereupon the customer said that he would report the attendant to his employer. The officer was on the point of leaving, when the attendant punched the customer in the face, knocking him to the ground.
>
> 32. Hilbery J held that the assault was not committed in the course of the attendant's employment, applying the Salmond formula. By the time that the assault happened the customer's business with the petrol station had ended, the petrol had been paid for and the customer had left the premises. When he returned with the police officer it was for the purpose of making a personal complaint about the attendant. The attendant reacted violently to being told that the customer was going to report him to his employer, but there was no basis for holding the employer vicariously liable for that behaviour. The judge was right to dismiss the customer's claim against the petrol company. At the time of the incident the relationship between the plaintiff and the attendant had changed from that of customer and representative of the petrol company to that of a person making a complaint to the police and the subject of the complaint. In *Lister v Hesley Hall Ltd* [2002] 1 AC 215 Lord Millett commented, at para 80, that "the better view may have been that the employer was not liable because it was no part of the duties of the pump attendant to keep order", but there is no suggestion in the report of the case that there was any other employee in practical charge of the forecourt and cash desk area. If the attendant had punched the customer because he believed, rightly or wrongly, that the customer was leaving without payment, I would regard such conduct as occurring within the course of his employment."

69. We agree with the analysis of Asplin LJ in the recent case of *Bellman v Northampton Recruitment Ltd* [2018] EWCA Civ 2214 that it was not so much the temporal gap between the attendant's argument with the customer and the assault which was significant in *Warren v Henlys* but rather the change in the nature of the relationship. As

Hilbery J said ([1948] 2 All ER 935 at 938E):-

> "It seems to me that it was an act entirely of personal vengeance. He was personally inflicting punishment, and intentionally inflicting punishment, on the Plaintiff because the Plaintiff proposed to take a step which might affect Beaumont in his own personal affairs. It had no connection whatever with the discharge of any duty for the Defendants. The act of assault by Beaumont was done by him in relation to a personal matter affecting his personal interests and there is no evidence that it was otherwise."

70. Ms Proops also submitted that the effect of the jurisprudence on vicarious liability is that the employer is only liable if the employee was "on the job" when the tort occurred. That is her phrase rather than a phrase found in the leading authorities, and we must bear in mind Lord Toulson's observation in *Mohamud* that the law would not be improved by a change of vocabulary. The same applies to her submission that vicarious liability only applies if the employee is seen to be acting in a representative function: a formulation which was expressly rejected by Lord Dyson JSC in *Mohamud* at [53].

71. It is no doubt true that, as Lord Clyde said in *Lister v Hesley Hall Ltd* [2002] 1 AC 215 at 235, the time and place at which the act or acts occurred will always be relevant, though not conclusive. Nevertheless, there are numerous cases in which employers have been held vicariously liable for torts committed away from the workplace. An example is the recent case of *Bellman v Northampton Recruitment Ltd,* to which we have already referred above. Mr Bellman was a sales manager for the Respondent recruitment firm. Mr Major was the firm's managing director. A Christmas party was organised. At its end, Mr Major arranged taxis to transport staff to a hotel where they continued drinking, with drinks mainly paid for by the company. After a couple of hours, an argument broke out about a new employee's placement and terms. Mr Major got cross and summoned staff to give them a long lecture on his authority. When Mr Bellman questioned Mr Major's decisions, he (Major) punched him (Bellman), causing brain damage. It was held by this Court, reversing the trial judge, that the defendant company was vicariously liable for the assault by the managing director.

72. In supplementary submissions on *Bellman,* the decision of this Court having been handed down the day after the hearing in the present case, Ms Proops argued that it supported her case that vicarious liability only applies if the employee was "on the job" when the tortious act was committed. We do not agree. The judgment of Asplin LJ does not use that phrase but rather refers at [24] to Lord Toulson, in *Mohamud,* having considered helpful the expression "within the field of activities assigned to the employee". The tortious acts of Mr Skelton in sending the claimants' data to third parties were in our view within the field of activities assigned to him by Morrisons.

73. We consider that the careful and detailed findings by the Judge at [184] of his judgment are a complete answer to this part of Ms Proops' argument:

> "… I reject Ms Proops' argument that the disclosure on the web of the payroll data was disconnected by time, place and nature from Skelton's employment. I find, rather, that as Mr Barnes submitted there was an unbroken thread that linked his work to

> the disclosure: what happened was a seamless and continuous sequence of events. My reasons for this are first that in October, prior to knowing he was again to be a conduit for payroll data between PeopleSoft and KPMG, Skelton showed signs of interest in the TOR network. When he knew (on 1st. November) that he was indeed to be the go-between, he obtained the mobile phone he was later to use just for making the criminal disclosures. He brought in a personal USB stick to work and copied payroll information to it in mid-November. Lying low for a while after that was necessary to create an appearance of separation and to avoid suspicion falling on him too readily. He again investigated TOR in December; adopted the user name and date of birth of a colleague to draw the blame onto him when setting up an account from which to upload the payroll data to the web; sent data to a web-sharing web-site in January, and either because that did not excite any great immediate interest, or because he had planned in advance to cause the maximum embarrassment to Morrisons immediately prior to the announcement of their financial results, sent the anonymous letters he did to three newspapers in March 2014. These actions were in my view all part of a plan, as the research and careful attempts to hide his tracks indicate. As I have already noted (para. 22 above) this is precisely the same view as that taken by HHJ Thomas QC when sentencing Skelton. This was no sequence of random events, but an unbroken chain beginning even before, but including, the first unlawful act of downloading data from his personal work computer to a personal USB stick."

74. The findings of primary fact in this paragraph are not in dispute. The Judge's evaluation of them in the opening and closing sentences of the paragraph as constituting a "seamless and continuous sequence" or "unbroken chain" of events is one with which we entirely agree. It is therefore unnecessary to embark on a discussion of the nature of the review by an appellate court of evaluative findings of this kind. In so far as the Judge's conclusions involved a value judgment (see *Dubai Aluminium Co Ltd v Salaam* [2003] 2 AC 366 per Lord Nicholls at [24]), it is one with which we agree.

75. Thus far, there is nothing unusual or novel in legal terms about this case, but there is one novel feature to it. We were not shown any other reported case in which the motive of the employee committing the wrongdoing was to harm his employer rather than to achieve some benefit for himself or to inflict injury on a third party. Ms Proops submitted that to impose vicarious liability on Morrisons in these circumstances would render the court an accessory in furthering Mr Skelton's criminal aims. As we said at [32] above, this was the point which troubled the Judge and which appears to have persuaded him to grant Morrisons permission to appeal.

76. Since the decision of the House of Lords in *Lloyd and Grace, Smith and Co* [1912] AC 716, which is the foundation of the modern law of vicarious liability, it has been clearly established that an employer may be vicariously liable for deliberate wrongdoing by an employee. In *Lloyd v Grace Smith* itself, the solicitor's clerk dishonestly procured a conveyance in his own favour of the client's property. His motive was greed. In the

sexual abuse cases such as *Lister v Hesley Hall Ltd* and the *Catholic Child Welfare Society* case the motive for the tort was sexual gratification. In *Mohamud* the motive of the foul-mouthed petrol pump attendant was personal racism rather than a desire to benefit his employer's business; but, said Lord Toulson, motive was irrelevant. Despite Ms Proops' submissions on this point, we do not accept that there is an exception to the irrelevance of motive where the motive is, by causing harm to a third party, to cause financial or reputational damage to the employer.

77. Ms Proops submitted that, given that there are 5,518 employees who are claimants in the present case, and the total number of employees whose confidential information was wrongly made public by Mr Skelton was nearly 100,000, this illustrates how enormous a burden a finding of vicarious liability in the present case will place on Morrisons and could place on other innocent employers in future cases. These arguments are unconvincing. As it happens Mr Skelton's nefarious activities involved the data of a very large number of employees although, so far as we are aware, none of them has suffered financial loss. But suppose he had misused the data so as to steal a large sum of money from one employee's bank account. If Morrisons' arguments are correct, then (save for any possible claim against the bank) such a victim would have no remedy except against Mr Skelton personally. Yet this hypothetical claimant would, as it seems to us, be in essentially the same position as Mrs Lloyd in *Lloyd v Grace, Smith.*

78. There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. We have not been told what the insurance position is in the present case, and of course it cannot affect the result. The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward by Ms Proops on behalf of Morrisons.

Conclusion

79. For these reasons we agree with the Judge that Morrisons was vicariously liable for the torts committed by Mr Skelton against the claimants. The appeal is dismissed.

……..

APPENDIX 1

THE DIRECTIVE

The following provisions of the Directive were mentioned in oral submissions before us.

Recitals

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is

recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes

or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller

for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

……

APPENDIX 2

THE DPA

1. Basic interpretative provisions

(1)In this Act, unless the context otherwise requires—

"data" means information which—

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

"data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

(2)In this Act, unless the context otherwise requires—

(a)"obtaining" or "recording", in relation to personal data, includes obtaining or recording the information to be contained in the data, and

(b)"using" or "disclosing", in relation to personal data, includes using or disclosing the information contained in the data.

4. The data protection principles

(1)References in this Act to the data protection principles are to the principles set out in Part I of Schedule 1.

(2)Those principles are to be interpreted in accordance with Part II of Schedule 1.

(3) ….

(4)Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

13. Compensation for failure to comply with certain requirements

(1)An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2)An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if—

(a)the individual also suffers damage by reason of the contravention, or

(b)the contravention relates to the processing of personal data for the special purposes.

(3)In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.

5 Unlawful obtaining etc. of personal data

(1)A person must not knowingly or recklessly, without the consent of the data controller—

(a)obtain or disclose personal data or the information contained in personal data, or

(b)procure the disclosure to another person of the information contained in personal data.

(2)Subsection (1) does not apply to a person who shows—

(a)that the obtaining, disclosing or procuring—

(i)was necessary for the purpose of preventing or detecting crime, or

(ii)was required or authorised by or under any enactment, by any rule of law or by the order of a court,

(b)that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,

(c)that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or

(d)that in the particular circumstances the obtaining, disclosing or procuring was justified

as being in the public interest.

(3)A person who contravenes subsection (1) is guilty of an offence.

(4)A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

(5)A person who offers to sell personal data is guilty of an offence if—

(a)he has obtained the data in contravention of subsection (1), or

(b)he subsequently obtains the data in contravention of that subsection.

(6)For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.

(7)Section 1(2) does not apply for the purposes of this section; and for the purposes of subsections (4) to (6), "personal data" includes information extracted from personal data.

(8)References in this section to personal data do not include references to personal data which by virtue of section 28 are exempt from this section.

SCHEDULE 1The data protection principles

Part I The principles

1Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a)at least one of the conditions in Schedule 2 is met, and

(b)in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Part II Interpretation of the principles in Part I

The first principle

1(1)In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2)Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who—

(a)is authorised by or under any enactment to supply it, or

(b)is required to supply it by or under any enactment or by any convention or other

instrument imposing an international obligation on the United Kingdom.

2(1)Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—

(a)in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and

(b)in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2)In sub-paragraph (1)(b) "the relevant time" means—

(a)the time when the data controller first processes the data, or

(b)in a case where at that time disclosure to a third party within a reasonable period is envisaged—

(i)if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

(ii)if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or

(iii)in any other case, the end of that period.

(3)The information referred to in sub-paragraph (1) is as follows, namely—

(a)the identity of the data controller,

(b)if he has nominated a representative for the purposes of this Act, the identity of that representative,

(c)the purpose or purposes for which the data are intended to be processed, and

(d)any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

The seventh principle

9Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a)the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b)the nature of the data to be protected.

10The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

(a)choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b)take reasonable steps to ensure compliance with those measures.