EFFECTIVE REDRESS OF GRIEVANCE IN DATA PROTECTION

An illusion?

MIKE VARNEY*

ABSTRACT

This article questions whether the current data protection legislative framework in the EU to provide effective redress of grievance for those who are affected by a breach of data protection law. It considers the extent to which the principle of effective judicial protection is satisfied where judicial redress is sought and also considers whether supervisory authorities are able to grant adequate administrative redress. In undertaking this analysis the article seeks to demonstrate that there are a number of areas where judicial protection is uncertain. There is a lack of consistency in the award of compensation, particularly in cases of non-pecuniary loss and some uncertainty as to what an 'effective remedy' might be in some data protection cases. Furthermore, substantial procedural differences exist between Member States for those seeking to bring data protection cases before national courts resulting in a situation where the conditions of access to judicial remedy are uneven.

Keywords: Data Protection; Grievance Redress; Remedies; European Union; Reform

§1. INTRODUCTION

Much focus has been placed on the role of data protection, given the predicted importance of innovation in online services and the use of personal data to economic growth and development in the European Union.[1] It is acknowledged that one vital aspect of the regime is the need to provide enhanced redress where data protection rules are violated.[2] Similarly, the provision of public services and many administrative and regulatory activities undertaken by public authorities or for public services require ever greater use of personal data and data exchange,

* Senior Lecturer at the University of Hull Law School, University of Hull, Hull, United Kingdom.
[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, COM(2012) 9 final, p. 2.
[2] Ibid., p. 6.

both within and outside the European Union.[3] Whether data is used by public bodies or organisations in the private sector, the need for public confidence in data processing systems will become increasingly important if there is to be public willingness to engage in further and more innovative use of data,[4] often shared not only within the borders of the European Union, but also outside.

The question which this article seeks to address is whether the existing framework of data protection legislation and its future reform will provide an effective system of grievance redress for those who have faced breaches of data protection rules. Such a system of grievance redress should focus not only on effective judicial protection, but also administrative regulation and methods of internal redress, offered by data controllers and processors.

The aims of this article are threefold. The first aim is to interrogate the concept of effective judicial protection in data protection cases. In the European Union, this may take two distinct angles. There is an issue of effective redress of grievance – that is, can the aggrieved citizen obtain an effective remedy? Furthermore, there is an issue of ensuring effective judicial protection throughout the Member States when a data breach occurs and redress is sought from a data controller in another Member State, or possibly even from a data controller outside of the European Union. The second objective of the article will be to consider whether effective protection is offered by the current legal regime. The third and final purpose of the article is to consider the steps that might be taken to address potential remaining gaps in protection.

§2. THE NATURE OF THE CHALLENGE

A. THE MANY LAYERS OF GRIEVANCE REDRESS IN DATA PROTECTION BREACHES

The right to protection of personal data is provided for in Articles 6 and 39 TEU, Article 16 TFEU and Article 8 of the EU Charter of Fundamental Rights. A more detailed framework of protection is provided for by secondary law, including the Data Protection Directive,[5] a Council Framework Decision on processing of data in matters of police and judicial cooperation[6] and further specific legislation on data protection in the use of electronic

[3] H.C.H. Hofmann, G.C. Rowe and A.H. Türk, *Administrative Law and Policy of the European Union* (Oxford University Press, 2011), p. 143-221.
[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, COM(2012) 9 final, p. 2.
[5] 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, [1995] OJ L 281/31.
[6] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L 350/60.

communications networks.[7] Each of these instruments require Member States to take steps to secure the rights set out in the legislation, with the Data Protection Directive and Framework Directive 2008/977/JHA creating an expectation that such rights may be secured in part by administrative authorities, but that judicial protection must always be available.[8]

In the case of the right contained in the TFEU and the right contained in the EU Charter of Fundamental Rights, there is a requirement of effective judicial protection as a result of Article 19(1) TEU and associated case law.[9] The right to effective judicial protection is further elucidated in Article 47 of the EU Charter of Fundamental Rights. In Europe, protection is further bolstered and to some degree complicated by the protection of personal data under Article 8 of the European Convention on Human Rights (ECHR) or the denial of an effective remedy for breach of Article 8 under Article 13 ECHR where it is found that states have failed to legislate appropriately to secure the protection of a claimant's privacy or personal data.[10]

Redress of grievance in data protection cases remains an important function of any effective system of data protection. Grievance redress could potentially come from three routes in the data protection sphere: the data controller may provide redress without reference to external intervention;[11] there could be intervention by the administrative authority responsible for the regulation of data protection in order to provide redress;[12] or there might be recourse to a court as envisaged by the Directive.[13] External to the data protection regime additional routes of redress might exist: for instance, individuals who suffer harm or loss as a result of a data breach might have the opportunity to bring proceedings in tort under national law for breach of data protection or privacy rights, if such claims are available,[14] or perhaps seek redress under the principle of just satisfaction under the ECHR.[15]

---

[7] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), [2009] OJ L 337/11.

[8] Directive 95/46/EC, Article 22; Council Framework Decision 2008/977/JHA, Article 20.

[9] Case C-222/84 *Johnston v. Chief Constable of the Royal Ulster Constabulary*, EU:C:1986:206; Case C-50/00 P *Unión de Pequeños Agricultores* v. *Council*, EU:C:2002:462.

[10] For an outline of some of the challenges in drawing distinctions between privacy and protection of personal data see J. Kokott and C. Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', 3 *International Data Privacy Law* (2013), p. 222.

[11] A fact acknowledged by legislation – Article 12 of Directive 95/46/EC creates a right of access to personal data for the data subject, combined with a right to require that data held which is incorrect be corrected. Article 14 of Directive 95/46/EC also requires that national law provides for a mechanism for data subjects to object to the processing of their personal data.

[12] As anticipated in Article 28 of Directive 95/46/EC, although it is notable that redress of grievance and provision of remedies to individuals is not the core thrust of Article 28.

[13] Directive 95/46/EC, Articles 22-24. Article 22 states that the judicial remedies are available '(…) without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28.'

[14] The position in respect of such rights varies across the Member States. See W. van Gerven, J. Lever and P. Larouche (eds.), *Tort Law: Cases, Materials, and Text on National, Supranational, and International Tort Law* (Hart Publishing, 2000), p. 141–169.

[15] This would be a difficult avenue to pursue for many claimants. For examples of successful claims for both pecuniary and non-pecuniary losses arising from issues relating to data protection see ECtHR, *K.U. v. Finland*, Judgment of 2 December 2008, Application No. 2872/02; ECtHR, *L.H. v. Latvia*, Judgment of 29 April 2014, Application No. 52019/07; ECtHR, *I v. Finland*, Judgment of 17 July 2008, Application No. 20511/03.

In data protection law, data protection cases are often dealt with initially by the data controller as a result of a complaint brought by an individual about an alleged violation of data protection law (whether a refusal of access to personal data or some kind of unlawful processing or release), proceeding to some formal intervention only if the response of the data controller fails to satisfy the aggrieved data subject. Should the data subject seek to pursue the breach further, a complaint might be considered by a supervisory authority before arising in a national court.[16] Other cases concerning data protection might arise through judicial review proceedings. Such actions may originate from radically different national procedures, with different rules of access to the court, costs and potential remedies.[17] In the context specifically of the Data Protection Directive, there is a further grievance redress procedure as Article 23 requires, apart from a right to judicial review, that data controllers be liable for any damage caused by unlawful processing or act incompatible with national provisions pursuant to the Directive, yet the Directive lays down no particular requirements as to the procedure for such actions.

B. THE CHALLENGES OF DESIGNING AN EFFECTIVE GRIEVANCE REDRESS SYSTEM IN DATA PROTECTION CASES

A step back may allow us to apprehend the provision of effective remedies in data protection cases as a form of grievance redress – something that has been a source of concern to administrative lawyers for many years.[18] Data collection, storage and processing, whether by public sector or private sector data controllers, would benefit from an effective system of grievance redress. The present approach in the Data Protection Directive appears to be focused primarily on judicial redress of grievance if resolution between data controller and subject is not possible. The availability of administrative redress in the form of monetary compensation to those who have suffered as a result of breaches of data protection law is not mandated by the Directive. It has been argued that the concept of administrative justice '(…) concerns the extent to which individuals affected by decisions are treated fairly and have the ability to ensure adequate redress of grievances.'[19] Much the same might be said of redress mechanisms in data protection – endeavour should be made to ensure adequate scope for the redress of grievance in the design of the system.

---

[16] For an example see *R (C) v. Northumberland County Council* [2015] EWHC 2134 (Admin), where the claimant had pursued the grievance regarding the holding of data before the Information Commissioner before having recourse to judicial review proceedings.

[17] See as an example from England and Wales *R (Hussain)* v. *Secretary of State for Justice* [2014] EWHC 4151 (Admin) where a claim was made for judicial review of a claimed failure to disclose data after a valid subject access request. This case was brought as a judicial review claim. Here, the claimant could, and perhaps should, have brought a claim under a statutory appeal process provided for in Section 7(9) Data Protection Act 1998. If a claimant wishes to seek compensation for a breach of data protection principles, then in England and Wales it is necessary to bring proceedings in private law which, as will be demonstrated below, brings additional cost and uncertainty.

[18] P. Birkinshaw, *Grievances, Remedies and the State* (2nd edition, Sweet & Maxwell, 1994). See also A. Gamble and R. Thomas, 'The Changing Context of Governance: Implications for Administration and Justice', in M. Adler (ed.), *Administrative Justice in Context* (Hart, 2010); P. Birkinshaw, Grievances, Remedies and the State: Revisited and Re-appraised', in M. Adler (ed.), *Administrative Justice in Context* (Hart, 2010).

[19] A. Gamble and R. Thomas, in M. Adler (ed.), *Administrative Justice in Context*, p. 19.

Designing systems of grievance redress is, in general, complex. Equality of access may pose a particular challenge, as Le Sueur notes in the context of administrative justice:

> For well-informed, resourced and legally represented individuals, [an] array of processes and institutions may provide opportunities for redress that is fine-tuned to the nature of the grievance (…). For less knowledgeable people who lack access to appropriate advice and funds to pay for it, the various mechanisms are likely to be confusing and mistakes may be made about where to take a grievance.[20]

This is true also in the specific context of data protection; the various paths to redress outlined above assume that the complainant is aware of the different redress mechanisms and is in a position to pursue them.

Furthermore, insofar as the Data Protection Directive and Framework Decision 2008/977/JHA may apply to third country nationals resident outside of the European Union, there is a significant question as to whether any recourse to judicial protection is possible. The same argument might be made where residents of EU Member States seek to pursue data controllers resident outside of the European Union.

In order to examine whether the existing legislation on data protection offers adequate potential for grievance redress the discussion will now move on to consider the operation of the current regime in order to determine whether an adequate system of redress has been provided and to identify any significant problems or omissions that exist in the current law.

§3. EFFECTIVE GRIEVANCE REDRESS – THE CURRENT REGIME

A. JUDICIAL REMEDIES

The requirement of 'effective judicial protection' is a complex issue. Arnull states that

> In theory, it applies to both the Union judicature and to the national courts of the Member States, but it is the latter which have so far been affected most profoundly by it. For them, it belongs to the body of principles they must apply when asked to uphold a right conferred on a litigant by Union law.[21]

The principle was first elucidated in the *Rewe*[22] case and has been adhered to by the CJEU since.[23] The principle has two core elements, those of equivalence and effectiveness. These concepts have been defined by the CJEU in

[20] A. Le Sueur, 'Designing Redress: Who Does It, How and Why?', 20 *Asia Pacific Law Review* (2012), p. 18–19.
[21] A. Arnull, 'The Principle of Effective Judicial Protection in EU law: An Unruly Horse?', 36 *E.L. Rev.* (2011), p. 51.
[22] Case C-33/76 *Rewe Zentralfinanz eG v. Landwirtschaftskammer für das Saarland*, EU:C:1976:188.
[23] For an account of the history of the development of the principle, see A. Arnull, 36 *E.L. Rev.* (2011), p. 52-53.

a similar fashion since the decision in *Rewe*, with a 2009 case affirming these principles in similar language to those in *Rewe*.[24] In *Danske Slagterier* the CJEU stated that:

> It is thus on the basis of the rules of national law on liability that the State must make reparation for the consequences of the loss or damage caused, provided that the conditions, including time-limits, for reparation of loss or damage laid down by national law are not less favourable than those relating to similar domestic claims (principle of equivalence) and are not so framed as to make it in practice impossible or excessively difficult to obtain reparation (principle of effectiveness).[25]

Apart from the general requirements imposed by the principle of effective judicial protection, in data protection cases, Article 22 of the Data Protection Directive requires that all individuals facing an infringement of their rights in data protection law are afforded a judicial remedy. In addition to this, Article 23 of the Directive requires that it must be possible for those who have faced a violation of their rights under the Directive to claim compensation from the data controller who has breached the provisions of the Directive. There is a further requirement in Article 24 of the Directive that there should be effective sanctions for those found to be in breach of the Directive, alongside the stipulation in Article 28(3) that the Supervisory Authority in each Member State must have the power to intervene where there are breaches and that the Supervisory Authority should be in a position to bring legal proceedings where there is a breach of national provisions in relation to data protection. Similar provisions, drawn from the wording of the Directive, are found in Framework Decision 2008/977/JHA.

Apart from respecting the procedural provisions mandated by the rules secondary law outlined above, national courts are also called to review their national procedural rules in light of the principles of equivalence and effectiveness. The determination of equivalence is not difficult in such cases. The national court in any case must determine whether the cause of action for vindication of a right flowing from EU law is '(…) similar as regards their purpose, cause of action and essential characteristics' to those in national law.[26] There are then two questions of effectiveness. The first is a requirement of procedural effectiveness drawn from *Rewe* and the associated case law – that is, a requirement that the procedural rules in place (limitation periods, time limits, rules governing access to relevant documents, and so on) do not serve as an excessive barrier to the obtaining of a remedy. There is then the question of whether or not national law provides for an appropriate and effective judicial remedy, liability and sanction for the purposes of Articles 22 to 24 respectively of Directive 95/46/EC.

[24] Case C-445/06 *Danske Slagterier*, EU:C:2009:178.
[25] Ibid., para. 31.
[26] Case C-63/08 *Pontin*, EU:C:2009:666, para. 45; Case C-591/10 *Littlewoods Retail and Others*, EU:C:2012:478, para. 31.

The question of what precisely is an effective remedy for a breach of data protection rules may be difficult to answer. In cases which have led to pecuniary loss, it is possible to offer compensation for the loss and the remedy is calculated on a fairly simple basis, though there is clearly a need to demonstrate that the breach led to the loss and provide some demonstrable evidence that the loss occurred.[27] However, in cases where there is non-material damage but no clear pecuniary loss, the determination of appropriate redress is often challenging. For example, English courts have often been relatively sceptical about claims for injury to feelings, awarding only nominal damages, yet European Union case law appears to demand something more.[28]

A further but related question is whether, insofar as the breach of data protection law also constitutes a breach of Article 8 ECHR, the remedy awarded accords with the principle of just satisfaction under the Convention. Case law suggests that the European Court of Human Rights (ECtHR) adopts a restrictive approach to the award of compensation for non-pecuniary loss in Article 8 cases concerning breach of data protection rules. The ECtHR has held that in cases where data is retained but not used contrary to Article 8 ECHR, the finding of an infringement of Article 8 is an adequate remedy.[29] By contrast, where there has been use or disclosure of the information, or the state has failed to put a framework in place to prevent unlawful use or to provide an effective remedy in such circumstances, some financial compensation has often been awarded, although the quantum of compensation is usually relatively small.[30] There is clear evidence of a dichotomy between the *Franchet* case in the General Court and the decisions of the ECtHR in the sense that the General Court suggested that some form of pecuniary remedy would be necessary in every case where an individual's data protection rights were infringed. When the interpretation of data protection law in the European Union courts is contrasted with the requirements of the European Convention as stated by the ECtHR, these differences create significant uncertainty over what precisely should constitute an 'effective remedy' for a breach of data protection law.

The Data Protection Directive also envisages that administrative remedies might be pursued by those who face a breach of their data protection rights and it is to this issue that the discussion now turns.

B. ADMINISTRATIVE REMEDIES

Questions of effectiveness and equivalence might also arise in relation to the administrative sanctions and remedies available to a Supervisory Authority in a Member State. Although this issue may fall outside the strict

[27] Case T-48/05 *Franchet and Byk v. Commission*, EU:T:2008:257.
[28] Ibid.
[29] ECtHR, *S and Marper v. United Kingdom*, Judgment of 4 December 2008, Application No. 30562/04 and 30566/04, para. 133; ECtHR, *Amann v. Switzerland*, Judgment of 16 February 2000, Application No. 27798/95.
[30] ECtHR, *Rotaru v. Romania*, Judgment of 4 May 2000, Application No. 28341/95 (50,000 French Francs); ECtHR, *Szulc v. Poland*, Judgment of 13 November 2012, Application No. 43932/08 (€ 5,000); ECtHR, *K.U. v. Finland* (€ 3,000).

parameters of the legal requirement of equivalence and effectiveness that applies to judicial protection, administrative remedies are likely to be the starting point in terms of protection for the vast majority of individuals in some Member States. This may be due to the potential cost of launching proceedings under data protection law or the possible need for legal advice or support in launching such an action. Under the provisions of the Data Protection Directive it appears that, while supervisory authorities do have the power to prevent unlawful data processing in cases brought by individuals or groups, or to issue fines for breaches of data protection law, no supervisory authority has the power to make an order for damages to be paid to the victim of an infringement.[31] This renders the level of grievance redress offered by supervisory authorities unsatisfactory, particularly in Member States where the launching of judicial proceedings for the recovery of damages is costly. While in some Member States additional non-judicial bodies exist which can assist claimants to pursue claims, the powers of these bodies are variable and only relatively few can award a compensatory remedy to a claimant.[32]

The powers of supervisory authorities and the level of support that they might provide to aggrieved citizens are important because even if it is not possible for the supervisory authority to provide a compensatory remedy to the individual, such authorities provide an important source of information and support to those who may have had their data protection rights infringed.[33] However, it is evident that there are significant differences in the resourcing of supervisory authorities in the Member States which are not explained solely by reference to the different populations that the authorities have to serve.[34] These differences may lead to a decrease in effectiveness in the information and support activities which these authorities may carry out, adding another hurdle to effective grievance redress.

Where an individual has recourse to a supervisory authority regarding a breach of data protection law established in another Member State, the current regime under the Data Protection Directive creates further obstacles to effective redress of grievances, especially in cross-border situations. The recent *Weltimmo* judgment[35] clarifies the powers of supervisory authorities where there may be a cross-border element to the data protection breach. The CJEU held that a supervisory authority in a Member State other than the one where the data controller is formally established can carry out an investigation into a possible data breach but, if in the course of the

[31] European Union Agency for Fundamental Rights, *Access to Data Protection Remedies in the EU Member States* (Publications Office of the European Union, 2013), p. 20-21. See also European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities* (Publications Office of the European Union, 2010).
[32] European Union Agency for Fundamental Rights, *Access to Data Protection Remedies in the EU Member States*, para. 2.1.
[33] Ibid., para. 3,4.
[34] See the outline of the resourcing of the various supervisory authorities in Article 29 Working Party, 'Sixteenth Report of the Article 29 Working Party on Data Protection', Ch. 2. There is further acknowledgment that some supervisory authorities lack sufficient resources in European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities*, para. 4.1.2.
[35] Case C-230/14 *Weltimmo*, EU:C:2015:639.

investigation, the supervisory authority determines that the data controller is established in another Member State and is thus subject to the law of that other Member State, it has no jurisdiction to impose a penalty.[36] The determination of the state of 'establishment' is not based purely on the state in which a data controller is legally registered. According to the CJEU, 'establishment' should include '(…) any real and effective activity — even a minimal one — exercised through stable arrangements.'[37] In the *Weltimmo* case the data controller was formally registered in Slovakia, but there was evidence of permanent activity, a representative of the company was based in Hungary and a significant aspect of the company's business was the creation of websites, written in Hungarian, for the purposes of selling properties in Hungary. These factors would seem to suggest that the Member State court which referred the case would be in a position to find that the company concerned was subject to Hungarian law and thus that the supervisory authority has jurisdiction to impose a penalty.[38] In circumstances where a supervisory authority concludes that it does not have jurisdiction to impose a penalty as the data controller cannot be said to be established in the supervisory authority's Member State, then it is necessary to seek assistance from the supervisory authority in the Member State which has jurisdiction. There are several problems arising out of this need for coordination between supervisory authorities.

First of all, the resources available to supervisory authorities vary significantly across Member States, which may create imperfections in the co-ordination process between supervisory authorities. Secondly, enforcement powers differ throughout Member States, leaving uncertainties about the ability to deliver a consistent remedial approach across Member States. It has also been noted that although Article 28(6) of the Data Protection Directive requires cooperation and coordination between supervisory authorities, it is clear that such coordination has not yet developed to the extent that it has in other fields, such as European competition law. Similarly, the Article 29 Working Party[39] has been criticized for its informality and lack of co-ordination in its investigative activities.[40] The legislative process for the creation of the Data Protection Regulation, discussed below, appears to acknowledge that co-ordination both internally within the European Union and with third country supervisory authorities in the field of data protection could be improved.

[36] Ibid., para. 52-60.
[37] Ibid., para. 31.
[38] Ibid., para. 41.
[39] The Article 29 Working Party is created by Article 29 of Directive 95/46/EC. Its purpose is to provide a group to facilitate coordination between the supervisory authorities for data protection matters in each of the Member States.
[40] D. Kloza and A. Mościbroda, 'Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law', 4 *International Data Privacy Law* (2014), p. 125–128.

C. THE CHALLENGE OF THIRD COUNTRY CROSS-BORDER DATA PROTECTION BREACHES

Data protection cases often have a cross-border element. One of the fundamental objectives of the Directive is to set down common standards for the keeping and processing of personal data throughout the European Union, with further acknowledgement that data is often kept and processed outside the European Union's borders. This issue is addressed by the Data Protection Directive in Articles 25 and 26,[41] but we can see that EU law has had to consider these issues carefully in a number of respects. The CJEU's *Schrems* decision, which found that the US Safe Harbor scheme was not sufficient to secure adequate protection of personal data because it applied only to those undertakings that adhered to it and also because public authorities in the USA were not bound by it, constitutes one instance of challenged posed by data transfers occurring between the EU and third countries. This decision demonstrates the need for suitable administrative and judicial controls in cases of third country data transfers, permitting supervisory authorities to review the suitability of data protection measures in third countries even where the Commission has adopted a Decision holding that the protection offered is adequate.[42]

Enforcement and remedies against data controllers based outside the European Union's borders are a complex issue because the characterization of any compensation awarded to individuals is likely to be key in determining its enforceability in third countries. If the compensation is viewed as a product of a civil wrong, then the likelihood of enforcement is far greater than if it is considered to be an administrative act.[43] A decision to issue a fine against a data controller in a third country would likely be characterized as an administrative penalty and is unlikely to be enforced by a court in another state as a matter of private international law in the absence of a bilateral treaty on enforcement, demonstrating a significant gap in protection for those who suffer data breaches.[44]

The discussion in the previous three subsections demonstrates that there are a number of challenges with the application of the right to effective judicial protection and effective redress of grievance when viewed through

[41] Articles 25 and 26 of Directive 95/46/EC set out the rules governing data transfers to third countries. Article 25 sets out the general rule that data must not be transferred to third countries unless an adequate level of protection for the data is guaranteed. Article 25 empowers the Commission to issue Decisions, setting out which third countries offer adequate protection. Article 26 contains the possible derogations from Article 25, setting out the circumstances where Member States can permit data transfers to third countries even where adequate protection of personal data is not guaranteed.

[42] Case C-362/14 *Schrems*, EU:C:2015:650.

[43] The UK courts have considered the potential scope to enforce monetary awards arising from public law acts in cases such as *Mbasogo v. Logo Ltd.* [2006] EWCA Civ 1370 and *Tasarruf Mevduati Sigorta Fonu v. Demirel* [2006] EWHC 3354 (Ch). Both of these cases suggest that private law claims brought on the basis of the exercise of a public law power will not be enforced. The Court of Appeal in Mbasogo's case also emphasised that the determination of whether such a claim was based on the exercise of a public law power was one for English law.

[44] J.D. McClean and V. Ruiz Abou-Nigm, *The Conflict of Laws* (Sweet & Maxwell, 2012), Ch. 3. See also O. Jansen (ed.), *Administrative Sanctions in the European Union* (Intersentia, 2013). For a more detailed consideration of the conflict of laws issues as they apply to foreign penal and administrative laws see F. Strebel, 'The Enforcement of Foreign Judgements and Foreign Public Law', 21 *Loy. LA Int'l & Comp. L. Rev.* (1999); W. Dodge, 'Breaking the Public Law Taboo', 43 *Harvard International Law Journal* (2002); J. Walker, 'Foreign Public Law and the Colour of Comity: What's the Difference between Friends?', 38 *Can. Bus. LJ* (2003).

the lens of data protection. Particular challenges arise from the scope of and measurement of quantum of damage in cases where there has been non-material damage and also in situations where an action needs to be brought against a data controller situated in a jurisdiction beyond the borders of the EU, although it has been demonstrated above that even within the borders of the EU the availability of remedies and enforcement powers, whether judicial or administrative, is not necessarily uniform. The discussion will now proceed to give some practical examples, drawn from the UK, of certain of the issues outlined above.

§4. THE PRACTICAL IMPACT OF UNCERTAINTIES AT THE EU LEVEL – EXAMPLES FROM UNITED KINGDOM LAW

A. COMPENSATION FOR NON-MATERIAL LOSS

The procedure for claiming a breach of the data protection principles and seeking a remedy from the court is subject to the principle of national procedural autonomy and is hence not laid down by the Data Protection Directive. In the United Kingdom, the Data Protection Act 1998 complies with Article 23 of the Directive through Section 13 of the Act, which states:

> (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.

This section illustrates one of the problems with the protection of individuals in a realm like data protection using a Directive. Section 13(2) of the Act requires that 'distress' is caused by the failure to comply with the data protection principles. In *Halliday*,[45] the judge at first instance awarded nominal damages of £ 1 for the failure to process his financial data according to the data protection principles. The Court of Appeal held that this did not accord with the assessment of the General Court in *Franchet* and reassessed the level of compensation at £ 750.[46] Arden LJ said 'I would accept as a general principle that, where an important European instrument such as data

[45] *Halliday v. Creation Consumer Finance Ltd* [2013] EWCA Civ 333.
[46] Ibid., para. 35.

protection has not been complied with, there ought to be an award, and it is to be expected that the complainant will be frustrated by the non-compliance.'[47]

While this case shows that national court might be inclined to re-assess their national rules to ensure an effective grievance redress in data protection, an issue that remains is that it is difficult in such cases to determine what is an adequate level of compensation in such cases. The courts in the United Kingdom (and presumably in most, if not all other Member States) deal with this issue on a case by case basis, though this may lead to substantially different outcomes depending upon which Member State a case is brought. On the whole, the English courts have sought a degree of inspiration from ECtHR case law when determining quantum in such cases, but this may not be the practice in other Member States. Another approach that was suggested to the court in *Halliday* was that there should be some inspiration drawn from the approach of the UK courts in cases of injury to feelings in discrimination law, where case law has set down broad guidelines as to what level of compensation might be appropriate dependant on the broad circumstances of the case at hand.[48]

In light of these challenges, one might see the attraction of the adoption of a Regulation in the field of data protection,[49] although even this does not escape the problem that ultimately the claims for compensation, grounds for which are set out in Article 77 of the Data Protection Regulation would still fall to be determined in Member State courts.

B. ENFORCEMENT OF DATA PROTECTION CLAIMS AGAINST DATA CONTROLLERS BASED IN THIRD COUNTRIES

The case of *Vidal-Hall v. Google*[50] arose as a result of the issue known as the 'Safari Workaround', whereby Google was able to collect personal data of users on Apple computers using a cookie without their consent. This data stored in the cookie was used to deliver targeted advertising and it is argued in the case that as part of this, third parties could see personal data of the owners of the computers concerned. In order to pursue Google in English courts for this alleged breach, the claimants needed to gain the permission of the court to serve a writ out of jurisdiction (that is, serve a writ on a claimant resident outside of the United Kingdom) under Rule 6.36 of the Civil Procedure Rules in England and Wales. Such permission could only be granted (in circumstances relevant

[47] Ibid.
[48] See *Vento v. Chief Constable of West Yorkshire Police* [2002] EWCA Civ 1871; [2003] I.C.R. 318.
[49] As in the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, and the legislative process discussed below. Now published as
[50] *Vidal-Hall v. Google* [2015] EWCA Civ 311; [2015] 3 W.L.R. 409.

to this case) where the claim was seeking an injunction preventing further misuse of private information and insofar as compensation is concerned, where the action is one in tort. This opened up two questions for English law. First, is a tort of the misuse of private information known to English law? The second question is then whether the right to receive compensation for 'distress' as defined in Section 13(2) of the Act could be claimed independently of any material loss and, if so, was this claim a tortious one or some kind of administrative penalty?

The former question of whether there is a tort of misuse of private information as alongside the tort of breach of confidence has been a long-running debate in English law. Until relatively recently, it was argued and held that there was no tort of misuse of private information in English law. However, recent authorities have begun to develop the concept.[51] The law is now in a position whereby in *OBG v. Allan*, Lord Nicholls said:

> As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some instances information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. Privacy can be invaded by further publication of information or photographs already disclosed to the public (…)[52]

As such, it was held that there was a potential claim in tort for the claimants and they were permitted to proceed and serve proceedings on the defendant overseas.

The latter issue was whether Section 13(2) permitted a claim for compensation for distress where there was no pecuniary loss. This issue had been considered in *Halliday*, discussed above, but in that case it was held that some pecuniary loss had been suffered by the claimant, so the damages could be awarded accordingly. In *Vidal-Hall*, it was accepted that no damage had arisen as a result of the breach – the claim was purely for non-material damage. The court held that the scheme introduced by Parliament, which required material loss in order for a claim in relation to non-material loss to proceed was contrary to the claimants' rights under the Charter of Fundamental Rights, so the section of the statute should be disapplied.[53] Furthermore, the court acknowledged that the scheme set out by Parliament is not compatible with Article 23 of the Data Protection Directive.[54] In their Section 13(2) claim, the claimants were not seeking compensation, but were using the claim to seek an injunction preventing Google's future use of their information.

[51] *Campbell v. News Group Newspapers* [2004] 2 AC 457.
[52] *OBG v. Allan* [2008] AC 1, para. 255.
[53] *Vidal-Hall v. Google* [2015] EWCA Civ 311, para. 104-105.
[54] Ibid., para. 94.

The purpose of the above discussion, though partly based on the proclivities of English law, serves to illustrate some important problems of characterization of claims and also demonstrates a way in which the United Kingdom had failed to implement the Data Protection Directive effectively into domestic law. The characterization of the claim – in particular, in a domestic legal system whether a breach of the data protection principles give rise to a cause of action in private law, could be crucial to the question of whether or not a claim can be served and enforced outside of the borders of the European Union.

C. JUDICIAL REVIEW CLAIMS AND DATA HELD AND PROCESSED BY PUBLIC AUTHORITIES

The Data Protection Directive's principles are mainly centred around the ability of individuals to bring claims in relation to their individual cases, with the exclude of claims brought to defend a more general public interest. The case in the UK of *R (C) v. Northumberland County Council*[55] serves to illustrate the problem. In this case, C had been successful in his individual claim to have the data about him and his family removed from the local authority's records, but had a broader objection to the local authority holding records on families where there had been child protection issues for a long period (in this case, 35 years). As such, he felt compelled to bring a claim for judicial review against the policy of the local authority. The claim here was unsuccessful, as it was argued that the holding of the data was for a legitimate pubic interest in child protection, but it demonstrates a potential weakness in the system. Public authorities may face individual claims to remove the data concerned from their records, but maintain a policy until it is successfully challenged through judicial review.[56] This process is costly in the UK and it is the general rule that should a claimant be unsuccessful in the claim then the claimant will bear the costs of the action.

Should an individual approach a public authority and seek to challenge the legality of the handling of his/her data, then means for seeking redress is via judicial review of the processing decision.[57] There is no other means of redress in such cases which is certain to lead to action on the part of the public authority, since a complaint to the Information Commissioner (the administrative body dealing with such matters in the United Kingdom) does not necessarily lead to an effective remedy for an aggrieved individual because the supervisory

[55] *R (C) v. Northumberland County Council* [2015] EWHC 2134 (Admin); [2015] B.L.G.R. 675.
[56] In other legal systems there may also be an interesting question of whether continuing to hold data constitutes an administrative 'act' or 'decision' which is amenable to judicial review.
[57] *R (Catt) v. Association of Chief Police Officers of England, Wales and Northern Ireland and another (Equality and Human Rights Commission and others intervening)* [2015] UKSC 9; [2015] A.C. 1065.

authority does not have the power to quash policy decisions of public bodies in relation to the holding or processing of data.

§5. THE GENERAL DATA PROTECTION REGULATION – EFFECTIVE REDRESS OF GRIEVANCE?

Agreement was reached on a compromise text for the General Data Protection Regulation on 15 December 2015.[58] One might hope that this Regulation will relieve some of the challenges outlined above as the direct applicability of the Regulation will have far greater potential to create a more uniform position throughout the Member States. There are also a number of more significant changes that will likely improve the position for those seeking redress of grievance.

For those seeking compensation for a data protection breach it will now be possible to pursue either a data controller or processor and, furthermore, the individual concerned will be able to pursue the controller or processor in breach either in the Member State where the controller or processor has establishment, or in the Member State where the claimant has habitual residence.[59] This is an improvement over the position in the Data Protection Directive, where Member States provided for recourse to courts in national law and were thus not empowered to provide for the pursuit of remedies in other Member States.

We can also see a considerable improvement in Article 80 of the General Data Protection Regulation, which provides that each Member State should provide a body to support those who have suffered a violation of data protection law in bringing a claim and, indeed, should be able to bring a claim on behalf of those who have suffered a breach of data protection law. This should assist claimants considerably in vindicating their rights in the absence of resources to pursue a claim.

These reforms do not address all the challenges outlined above. In particular, there is still no requirement that supervisory authorities are able to provide compensation and, furthermore, there is nothing in the Data Protection Regulation outlining the principles which should apply when determining the quantum of the award for non-material damage.

[58] For the compromise text of the General Data Protection Regulation, see Note of the Council of the European Union, ST 15039/15 INIT. The Regulation is now published as Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/1.

[59] The only exception to this is where the claim is against a public authority exercising its public powers, when the claim must be instituted in the Member State of the public authority concerned.

The Data Protection Regulation also makes some significant improvements to the approach to administrative regulation of data protection. There is provision in Article 68 of the Regulation for a new regulatory agency at the European level – the European Data Protection Board. This body should improve the consistency of application of data protection law in the European Union as it has the power to issue opinions and create guidelines on the application of the law either on its own initiative, or if requested by a Member State supervisory authority.[60]

In addition, the Regulation provides for a clearer and more consistent framework for the issuing of administrative fines and other penalties, which presently differ somewhat between Member States.[61] Each of these measures recognize the increasing likelihood of cross-border infringements in the European Union and appear to be designed to create greater consistency in the approach to sanctions.

The Data Protection Regulation is also notable in its clearer approach to the jurisdiction of and co-operation between supervisory authorities. Article 55 of the Regulation sets out the principle that each supervisory authority is responsible for the activities of data controllers and processors on the territory of its own Member State, but the co-operation mechanism is now more clearly set out in circumstances where there is cross-border processing akin to that in *Weltimmo*,[62] discussed above. The General Data Protection Regulation provides that where there are cross-border issues, the supervisory authority in the Member State of main or single establishment retains a leading role in investigation and enforcement,[63] but there is explicit provision for a supervisory authority in another Member State to deal with complaints which are isolated to an establishment in its Member State, or substantially affects only residents in its Member State.[64] There is also a much improved and clarified mechanism of co-operation between supervisory authorities, replacing the more ad hoc arrangements in the Article 29 Working Party in the Data Protection Directive. This will likely improve the position of those who face a cross border data breach within the borders of the EU.

The position in regard to transfers of data to third countries is less clear. Chapter V of the General Data Protection Regulation deals for the approval of such transfers by a Decision of the Commission, where the data processor or controller ensures that there are adequate safeguards, or where binding corporate rules are in place to protect those whose data is transferred. In all of these circumstances the Data Protection Regulation refers to the provision of adequate remedies and complaints procedures, but the requirements are not specified with the

[60] Regulation 2016/679/EU, Article 70(1)(e).
[61] Ibid., Articles 83 and 84.
[62] Case C-230/14 *Weltimmo*.
[63] Regulation 2016/679/EU, Article 56(1).
[64] Regulation 2016/679/EU, Article 56(2).

same degree of precision as for data transfer and processing within the borders of the EU. However, one can see from the recently adopted US-EU Privacy Shield that there is a desire to provide a similar level of protection to that which exists in the Regulation, with the potential for alternative methods of grievance redress, reference to the Federal Trade Commission and judicial remedies all provided for in the agreement.[65] However, the Data Protection Regulation does not necessarily mandate this in all future agreements between the Commission and third countries, although the decision of the CJEU in *Schrems*[66] is likely to continue to resonate in all future international agreements and will thus provide much greater harmonization and access to dispute resolution and remedies for aggrieved parties.

§6. CONCLUSION

This article has sought to stress the need for effective redress of grievance in data protection law. This does not necessarily require a judicial remedy in all circumstances and, indeed, in many cases a judicial remedy may not be the most effective route to redress. The discussion has sought to emphasise the existing weaknesses in the provision of effective remedies, whether judicial or administrative, under the Data Protection Directive, some of which have been further illustrated by reference to UK law. Particular weaknesses in consistency of application of the law, uncertainties over the precise scope and availability of remedies, particularly for non-material loss and challenges over the jurisdiction of and co-operation between supervisory authorities exist. Given the continuing growth of the use of personal data in new and innovative ways and the growth of cross-border use of data in particular, these weaknesses lead to a significant number of gaps in effective redress of grievance in data protection cases.

The Data Protection Regulation will address a number of these issues provided that the grievance arises as a result of processing of data within the borders of the European Union, although the position with regard to compensation for individuals remains unclear. The most pressing difficulties and uncertainties that remain in terms of grievance redress exist predominantly in the interface between the European Union and third countries. However, the EU-US Privacy Shield agreement demonstrates that here the CJEU has had considerable impact in its *Schrems*[67] decision in creating certain clear rights that EU citizens might expect in all situations where data is shared with third countries. One might regard this as a 'constitutionalization' of such rights, requiring that any

[65] Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final.
[66] Case C-362/14 *Schrems*.
[67] Case C-362/14 *Schrems*.

agreement between the European Union and a third country secures these rights. However, it is far more challenging to ensure that redress of grievance is effective when negotiating an agreement with a third country, as the procedural steps necessary for securing such redress, the approach of the courts to awarding compensation and the resources available to supervisory authorities may all be significantly different to those which exist in the European Union. This issue is unlikely to be addressed unless there is progress towards stronger international standards on data protection and greater international harmonization of remedies in such cases.