

# FEATURED PERSPECTIVE

## Privacy Rights in an Age of Transparency: A European Perspective

by Philip Baker



Philip Baker QC is with Field Court Tax Chambers in Gray's Inn in London.

This article is based on a presentation at the International Conference on Taxpayer Rights in Washington on November 18-19, 2015.

In this article, the author addresses taxpayer privacy and data protection issues in Europe, examining how automatic exchange of taxpayer information could infringe upon rights to confidentiality and privacy.

**T**hroughout the rapid development of systems for automatically exchanging financial information for tax purposes, inadequate attention has been paid to data protection rules for preserving privacy and confidentiality. This article aims to address this oversight, providing a European legal perspective on taxpayers' rights in an age of transparency.

### Automatic Exchange of Information

Provisions for the exchange of information between tax authorities have been in place for over a century. One of the earliest such models, prepared by the League of Nations in the 1920s, provided for administrative cooperation between tax authorities. Since the late 1950s, the vast majority of tax treaties based on the OECD draft and model and the U.N. model have provided for information to be exchanged on request, spontaneously, and automatically. Substantial amounts of some types of data have been subject to automatic exchange for decades. On a broader scale, the Council

of Europe/OECD Multilateral Convention on Mutual Administrative Assistance in Tax Matters, which now has over 90 signatories, contained equivalent provisions for exchange on request and automatically.

Within the European Union, the Directive on Administrative Cooperation in Tax Matters has been in place since 1977, beginning as Council Directive 77/799/EEC of December 9, 1977, before being redrafted and replaced with Council Directive 2011/16/EU (the DAC) in 2011. This directive also provided for exchange of information on request and automatically.

The main impetus for moving toward automatic exchange came from revelations in the mid-2000s concerning undisclosed foreign bank accounts held by U.S. citizens, mainly in Switzerland. This led the U.S. Congress to pass the Foreign Account Tax Compliance Act, which required foreign financial institutions to identify accounts held by or for U.S. citizens and supply that information to the U.S. administration. Due to fears that confidentiality obligations in some countries would be breached if information were supplied by financial institutions directly, a network of intergovernmental agreements was concluded to allow foreign governments to supply the information to the U.S. Spotting an opportunity to use this development to their advantage, the U.K. and several other European countries began concluding FATCA-like IGAs with various jurisdictions, including U.K. crown dependencies and overseas territories.

By the summer of 2013, it was clear that a new international standard for cooperation between revenue authorities had emerged based upon automatic exchange of financial account information. Within the OECD, this was implemented through a common reporting standard (CRS) for automatic exchange of financial account information, approved by the OECD Council on July 15, 2013, and endorsed by the G-20 shortly afterward. Meanwhile, the EU Council of

Finance Ministers reached a political agreement in October 2014 to extend the DAC to include automatic exchange of financial account information. This agreement was implemented by Directive 2014/107/EU of December 9, 2014, which was followed by a tax transparency package in March 2015 that has led to further amendments to the DAC.

The directive requires all EU member states to implement automatic exchange of financial information. For non-EU states, the provisions for automatic exchange of information (AEI) in bilateral treaties and in the multilateral administrative assistance convention require implementation via a competent authority agreement. On October 29, 2014, a multilateral competent authority agreement was signed to give effect to automatic exchange of financial information in accordance with the CRS. A group of “early adopter” countries will begin exchanging information under the agreement from September 2017.

The DAC and the CRS are similar in their general approaches, though they differ on the details. The U.S. has indicated that it does not intend to adopt the CRS at this time and will continue following the FATCA arrangements, which differ from the DAC/CRS in many respects.

The situation has therefore moved very far and fast from limited exchange of information between revenue authorities on request to widespread, automatic exchange of financial account information between governments. Although several different systems for exchange exist, most countries will, in practice, operate based on FATCA with the U.S. and DAC/CRS with the rest of the world.

In this headlong rush toward automatic exchange of financial account information, very little attention appears to have been paid to instituting the necessary safeguards for taxpayers’ rights to confidentiality, privacy, and data protection. Although countries undoubtedly enter into AEI arrangements for tax purposes, no source authorizes tax administrations to disregard taxpayers’ rights in implementing those arrangements.

## European Privacy and Data Protection Rights

### Privacy and Confidentiality

The starting point for a discussion of taxpayers’ rights in connection with AEI is article 8 of the European Convention on Human Rights (ECHR). Article 8 enshrines the right to respect for private and family life, providing as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is *in accordance with the law* and is *necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for*

the protection of health or morals, or for the protection of the rights and freedoms of others. [Emphasis added.]

A parallel provision is found in article 7 of the Charter of Fundamental Rights of the European Union.

There is an increasing body of jurisprudence on the application of the article 8 right to privacy to the gathering and exchange of information between tax authorities. In an early case before the European Commission on Human Rights,<sup>1</sup> *X (Hardy-Spirlet) v. Belgium* (decision of December 7, 1982), it was held that the gathering of information on a taxpayer by a revenue authority prima facie breached the right to privacy under article 8. Such a breach could be justified only if it was in accordance with the law, necessary in a democratic society, and proportionate. This reasoning was followed in one of the leading cases decided by the European Court of Human Rights (ECtHR), *Funke v. France* (Appln. No. 10828/84, February 25, 1993).

Several more recent cases have involved challenges to the exchange of information. In *FS v. Germany* (Appln. No. 30128/96, November 27, 1996) the ECtHR held that exchange of information between Austria and Germany under the DAC was lawful and proportionate. In deciding whether taxpayers have a right to review information gathered from a foreign state, the ECtHR in *Janyr v. Czech Republic* (Appln. No. 42937/08, October 31, 2013) found the taxpayer had received a fair trial, even though information was only partially obtained from a foreign jurisdiction. Finally, in *Jiri Sabou v. Czech Republic*, C-276/12 (CJEU 2013), the Court of Justice of the European Union dealt with whether a taxpayer had a right to participate in formulating questions and examining witnesses in a dispute over the financial information that was exchanged between states. The CJEU held that information gathering was an essentially administrative procedure and did not necessarily require fair trial rights to be protected.

In summary, collection, retention, and exchange of information between tax authorities is prima facie a breach of the right to privacy in article 8 of the ECHR and article 7 of the EU Charter. Such practices may be lawful, however, if they are carried out in accordance with the law and necessary in a democratic society (so that there is a fair balance between the rights of the individual and those of the state) and the information gathering is proportionate. Although rights-based challenges to information exchange are unlikely to succeed, tax authorities within the Council of Europe must respect fundamental rights when legislating and implementing measures for such practices.

<sup>1</sup>Until the entry into force of Protocol 11 of the ECHR in 1988, individuals did not have direct access to the European Court of Human Rights; they had to apply first to the (now defunct) European Commission on Human Rights.

## Data Protection

When the ECHR was drafted in the late 1940s, the idea of gathering and exchanging large amounts of electronic data could hardly have been foreseen. Consequently, the ECHR contains no specific protection relating to the processing of data. Under EU law, however, data protection is explicitly addressed by several sources, including the treaties establishing the EU. Article 16 of the Treaty on the Functioning of the European Union (TFEU), for example, provides as follows:

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

Similarly, the EU Charter on Fundamental Rights contains an explicit provision on data protection in article 8, which provides:

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

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

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

Data protection is also addressed in Directive 95/46/EC (the “Data Protection Directive”), which will be replaced by a General Data Protection Regulation within the next few months. The Data Protection Directive grants very specific rights to individuals whose personal data is subject to any form of processing. Article 11, for example, proclaims that the data subject has a right to know that data on him are being collected, while article 12 enshrines the right to access the data and rectify any inaccuracies. Under article 23, the data subject has a right to compensation for any unlawful processing of data. The directive also contains specific provisions addressing the transfer of personal data to third countries (that is, non-EU member states). Article 25 requires that “the transfer to a third country of personal data . . . may only take place if . . . the third country in question ensures an adequate level of protection.”

The protection of data processed in the EU is overseen by a working party established under article 29 of the directive, which consists of representatives from all

member states. The working party has, on a number of occasions, expressed its concern over the insufficient data protection safeguards in place in connection with the AEI for tax purposes. Thus, in a June 21, 2012, letter discussing the application of data protection to FATCA, the working party stated that it:

shares the concerns expressed by some in relation to dual compliance with FATCA and the Directive. Without an appropriate legal basis justifying both sets of obligations imposed on European FFIs would result in the unlawful processing of personal data.

Similarly, in a September 18, 2014, letter on the CRS, the working party observed that:

The practical roll-out of CRS in Europe based on existing FATCA IT solutions currently lacks adequate data protection safeguards, notwithstanding the EU proposal to amend the Directive 2011/16/EU regarding mandatory automatic exchange of information in the field of taxation. This Directive — which could be considered as transposition of the US FATCA and CRS in EU law — so far falls short of data protection safeguards.

The working party established under the Data Protection Directive has therefore warned on several occasions that the safeguards built into the AEI arrangements are inadequate.

The concerns of data protection officials are most clearly reflected in an amendment to the DAC made in December 2014 under article 1(5) of Council Directive 2014/107/EU. The amendment inserted the following wording into the DAC:

2. Reporting Financial Institutions and the competent authorities of each Member State shall be considered to be data controllers for the purposes of Directive 95/46/EC.

3. Notwithstanding paragraph 1, each Member State shall ensure that each Reporting Financial Institution under its jurisdiction *informs each individual Reportable Person* concerned that the information relating to him referred to in Article 8(3a) will be collected and transferred in accordance with this Directive and shall ensure that the Reporting Financial Institution provides to that individual all information that he is entitled to under its domestic legislation implementing Directive 95/46/EC *in sufficient time for the individual to exercise his data protection rights* and, in any case, before the Reporting Financial Institution concerned reports the information referred to in Article 8(3a) to the competent authority of its Member State of residence.

4. Information processed in accordance with this Directive shall be retained for no longer than necessary to achieve the purposes of this Directive,

and in any case in accordance with each data controller's domestic rules on statute of limitations. [Emphasis added.]

This is a critical change for EU member states. Under the new wording, data protection rules apply to both the financial institutions gathering information for the purpose of automatic exchange and the competent authorities of each member state responsible for carrying out the automatic exchange. Each reporting financial institution is explicitly required to inform the data subject that information will be collected and transferred and to do so in sufficient time for the individual to exercise his data protection rights (including the right to examine the data being transferred and rectify any inaccuracies). As financial institutions in Europe begin gathering information for the purposes of FATCA or the CRS over the next year, they will therefore have to notify the data subjects that information on them is being gathered and exchanged.

Data protection is not simply about the confidentiality of the data being gathered and exchanged. Keeping the information confidential and guarding against unauthorized disclosures is simply the starting point. Foreign tax authorities that make inadequate provisions for guaranteeing the confidentiality of data and are prone to data leaks are clearly offering substandard data protection and cannot possibly receive data by way of automatic exchange until these safeguards are bolstered.

Confidentiality is just the baseline, however; data protection law gives the data subject far more extensive rights. Data may be gathered and exchanged only for a lawful purpose that must be clearly identified in specific terms so that any misuse of the data can be challenged, and it must not be retained longer than neces-

sary for the identified purpose. The data subject has the right to be notified, to access the data, and to correct any inaccuracies. Legal remedies must be put in place to protect the rights of data subjects, and compensation must be paid to them for any improper data processing.

Data protection rights therefore go well beyond just ensuring confidentiality. This is perhaps the most important lesson to draw from the European protection of privacy, confidentiality, and data protection with regard to AEI. These rights, however, are likely to lead to a range of challenges once the AEI systems begin to operate and raise a whole series of practical questions. How will these data protection provisions operate in practice alongside AEI? Now that the purpose for gathering and exchanging information must be identified, how will permissible purposes be defined, and how can unlawful use be challenged? Is taxpayer profiling an allowable use of information? For how long can the data be retained before it must be destroyed? How will countries with inadequate data protection provisions be identified, and how will the international community react when those countries refuse to exchange information? What will happen when (as is almost inevitable) data exchanged under these systems are leaked? Will the whole system be vulnerable to destructive challenge?

Developments in data protection are expected to take place very rapidly. The CJEU has struck down entire legislative arrangements on information processing due to inadequate protections therein. Large parts of the edifice being erected for AEI could be struck down because the authorities concerned have, in their haste to establish a system for exchange, failed to respect taxpayers' rights. ◆