Analysis

HMRC challenged over CRS information exchange rules

Speed read

An EU national has made a complaint to the UK Information Commissioner's Office about HMRC and the UK's adoption of the common reporting standard (CRS) on the basis that her privacy and data protection rights are being infringed. Some parallels can be drawn with the successful challenge to the EU Data Retention Directive on grounds that it was not compatible with the fundamental rights to privacy and the protection of personal data set out in the EU Charter of Fundamental Rights. However, the position in relation to CRS can be distinguished in various respects, such that it would not appear as soft a target as the Data Retention Directive. Nevertheless, if successful, the challenge would strike a major blow to CRS and potentially stem the tide of other broad transparency measures involving personal data, at least within the EU.

Hatice Ismail
Simmons & Simmons
Hatice Ismail is a corporate tax partner at Simmons & Simmons LLP. She advises on all aspects of corporate tax, including corporate, restructuring, structured finance, cross-border and real estate transactions, predominantly for clients in the asset management and investment funds and financial institutions sectors. She also advises on stamp taxes, VAT and international automatic exchange of tax information regimes. Email: hatice.ismail@simmons-simmons.com; tel: 020 7825 3977.

The common reporting standard (CRS) is under attack. An EU national has made a complaint to the UK data protection regulator, the Information Commissioner's Office (ICO), copying in the EU data protection authorities, about HMRC and its implementation of the CRS. The CRS is an automatic exchange of information regime, which so far more than 100 jurisdictions have implemented under local law, with the aim of combating tax evasion. It was developed by the Organisation for Economic Cooperation and Development (OECD) at the request of the G20 and is modelled on the US Foreign Account Tax Compliance Act (FATCA) regime.

Under CRS, financial institutions are required on an annual basis to electronically report to their local tax authorities information about 'financial accounts' held by foreign resident taxpayers. This information is then automatically electronically exchanged with the tax authorities in the jurisdiction(s) in which the taxpayer is resident (if the jurisdiction is a CRS reportable jurisdiction). The CRS information collected and exchanged includes personal information enabling the identification of the taxpayer (such as name, address, date/place of birth and tax identification number) and financial account details (including account number, calendar year end account balance or value, and gross payments paid or credited to the account during the year). It can also extend in certain circumstances to such information about the ultimate controlling persons of the direct account holder.

The individual complainant is believed to be an Italian resident maintaining a UK bank account with a small balance that falls within the scope of CRS reporting to the Italian tax authorities via her bank and HMRC. She is apparently claiming that CRS makes her personal information vulnerable to cyber hacking or loss and infringes both the EU General Data Protection Regulation (GDPR) (which took effect across the EU in May 2018) and human rights laws.

Under article 8 of the European Convention of Human Rights, incorporated into UK law by the Human Rights Act 1998, everyone has the right to respect for his private and family life, home and communications. The EU Charter of Fundamental Rights (the European Charter), which is even broader, applies across the EU and includes the fundamental rights to privacy and protection of personal data. None of these rights are absolute; they are qualified by the ability of public authorities to interfere with these rights where such interference is in accordance with the law, is necessary in a democratic society and is proportionate to meet certain kinds of legitimate aims, such as to protect the economic wellbeing of the country or prevent crime (e.g. tax evasion). The protection of the right to privacy and data protection go to the heart of the GDPR rules, which are aimed at giving individuals more control over their personal data.

No doubt the individual's challenge centres around the view that CRS goes beyond what is necessary and proportionate to meet its stated objective of combating tax evasion by taxpayers that hold overseas accounts or investments. We have not seen the details of the complaint but are aware of the views of the individual's legal counsel, Mishcon de Reya LLP.

Where would a successful challenge leave the trend for transparency related measures?

If successful, the challenge would strike a major blow to CRS and potentially stem the tide of other broad transparency measures involving personal data, at least within the EU. A simultaneous complaint on similar grounds was also raised in relation to beneficial ownership registers.

The ICO has the power to impose temporary or permanent limits on the processing of personal data where it finds that GDPR rules are being infringed. It is unclear where the use of such enforcement powers would leave the UK, and HMRC as a 'data controller' for CRS purposes, in connection with meeting its CRS information exchange obligations under bilateral and multilateral agreements with numerous jurisdictions and under the EU directive on the EU wide implementation of CRS, known as 'DAC2'. More generally, it would also leave the CRS/DAC2 vulnerable to further challenge in the courts at EU level.

The GDPR rules are underpinned by the fundamental rights to privacy and data protection, and require those rights to be respected in applying any local law derogations from the rules. In post-Brexit Britain, these rules will remain in effect, even if the European Charter of Fundamental Rights is no longer part of UK law from Brexit day and the UK government were to cease to be a signatory to the European Convention on Human Rights and repeal the UK Human Rights Act 1998 (which is not expected to occur during the current Parliament). The Data Protection Act 2018 secures the application of the GDPR in a post-Brexit Britain.

Could the challenge pave the way for CRS to be struck down altogether?

There is precedent for a challenge on similar grounds succeeding. In 2014, the CJEU held, in *Digital Rights Ireland* and *Seitlinger and Others* (joined cases C-293/12 and C-594/12), following references from Austrian and Irish courts, that the Data Retention Directive (2006/24/EC) was invalid on the basis that the interference it caused with the fundamental rights of privacy and protection of data laid out in the European Charter was disproportionate, and the court also raised data security concerns. That directive required member states to adopt laws requiring electronic communications service providers to retain certain types of traffic, location and subscriber generated data for a period of between six and 24 months to enable the data to be available for the purposes of the investigation, detection and prosecution of serious crime by public authorities and law enforcement authorities. Although the directive had a legitimate aim (i.e. the investigation, detection and prosecution of serious crime), its provisions were held to be a disproportionate restriction on the rights of individuals to privacy and the protection of their personal data. The CJEU particularly criticised the following aspects of the directive:

- The data retention provisions compromised the essence of the fundamental right to a private life without being limited to what was strictly necessary as they affected almost all EU citizens and means of electronic communication in a general and comprehensive manner, without any differentiation, limitation or exception, and without a link between the behaviour of an individual and serious crime.
- The directive did not restrict access to and use of the data for strictly law enforcement and public security reasons.
- The directive did not require access to the data to be subject to prior independent review by a court or other administrative body.
- The directive did not ensure compliance with data security requirements, as it did not require the retention of the data within the EU, impose specific safeguards to ensure effective protection of the data against the risk of abuse and unlawful access and use, or ensure the irreversible destruction of the data at the end of the retention period.

Some parallels can be drawn between the kinds of issues that contributed to the CJEU's ruling that the EU Retention Directive was not compatible with the EU charter on fundamental rights to privacy and the protection of personal data, and findings in later relevant cases, and the CRS/DAC2 regime (including as implemented in the UK). However, the position in relation to CRS/DAC2 is less clear cut and can be distinguished in various respects.

How vulnerable is the CRS regime?

The CRS/DAC2 does require the exchange of certain information on a broad range of people with the aim of detecting and preventing tax evasion. However, the scope of the reporting is not without limitation or exception, as the reporting is generally limited to cover taxpayers resident in 'reportable jurisdictions' and is subject to exceptions relating to certain perceived low risk categories of financial account holders and types of financial account. Unlike under FATCA, there is generally no materiality or 'de minimis' threshold to weed out low value/balance accounts; however, the rationale for this is to prevent the reporting rules being circumvented through the use of multiple low value/balance accounts with different financial institutions.

The information reported is arguably not sufficiently aligned with a taxpayer's actual obligation to pay tax in its home jurisdiction in relation to its relevant overseas financial accounts; nor is it linked to any circumstances or behaviour that indicates that tax is actually being evaded. However, it would not be possible to require a financial institution to understand and report on the basis of an overseas investor/customer's specific tax obligations and tax position. Indeed, any attempt to require such an approach to be taken would inevitably be more intrusive to investors/customers that hold the financial accounts.

This does mean that there is scope for reports to be made that are essentially 'false positives' because the payments made to, and the account balance/value of, the financial account do not equate to taxable income or gains of the taxpayer reported on. An extreme example of this includes a passive entity's financial accounts, where the individual controlling persons are required to be identified and reported on if resident in a reportable jurisdiction and the only such identifiable person is the 'senior managing official' (such as the managing director), who is unlikely to owe tax in respect of the financial account.

Some parallels can be drawn between the kinds of issues that contributed to the CJEU's ruling that the EU Retention Directive was not compatible with the EU charter on fundamental rights to privacy and the protection of personal data

The CRS reportable information is modelled on FATCA, which was designed to be aligned to US tax obligations and not the varied local tax obligations applicable in participating jurisdictions; however, the information reported could be viewed as sufficiently limited and necessary for the purposes of the legitimate aims of the measures. In particular, it is difficult to see reporting of income and redemption/sale proceeds as excessive or irrelevant to any local tax regime. Even if the account balance or value reportable is not connected to a specific tax liability (because the taxpayer reported on is not resident in a jurisdiction that levies a wealth tax), this information is still relevant for the purposes of ensuring that capital is not hidden overseas, even if that capital is not immediately taxable.

Although the CRS regime applies to financial accounts irrespective of any suspicions of any tax evasion, the regime at least excludes low risk financial account holders and accounts. Without tax authorities using CRS to learn of the existence of overseas financial accounts, it is difficult to see how such a suspicion of related tax evasion could arise except in a very small number of cases.

The CRS regime needs to be broad in nature and scope to achieve its intended objective. Blanket privacy facilitates tax evasion; and arguably the previous or other existing regimes that enable tax authorities to obtain information about overseas financial accounts are

too limited in scale to have the kind of impact that tax authorities and the public seem to want in curbing tax evasion, especially by high net worth individuals.

It might be an attractive proposition for champions of privacy to argue that CRS/DAC2 must be disproportionate because it is not squarely aligned with the domestic tax rules in all of the reportable jurisdictions. Some allowance must be made, though, for the global nature and need for consistent implementation of the regime, and the limitations to its scope, notwithstanding that it is an imperfect regime and creates the potential for 'false positive' reports to be made in accordance with the law that could lead to enquiries for the taxpayer from its local tax authorities.

If a lack of a suspicion of wrongdoing of taxpayers were the main hurdle to meeting the principle of proportionality, then surely the FATCA regime should be the first to fall. Indeed, using financial institutions to help in the fight against tax evasion would be entirely the wrong weapon.

What about safeguards for taxpayers of their data in relation to CRS/DAC2?

Whether or not they go far enough, there are data protection safeguards built into the CRS regime, including DAC2 and the UK implementation rules.

Whichever treaty or exchange of information instrument is used to require one jurisdiction to exchange CRS information with another, that legal instrument will include provisions on confidentiality and specifically limit the use of the data exchanged to those agreed by the jurisdictions (e.g. tax administration). HMRC states in its *International Exchange of Information Manual* that it only exchanges information with other tax administrations under the legal instruments for tax administration purposes, unless special permission is sought to use the data for other purposes. Such permission will only be granted for another law enforcement purpose if there is an equivalent legal gateway to pass the data to a similar law enforcement body.

The CRS multilateral competent authority agreement, signed by over 100 jurisdictions to date, provides that all information exchanged is subject to the confidentiality rules and data safeguards provided for in the relevant legal instrument, including if necessary safeguards that are required by domestic law. It provides that each jurisdiction will notify the other immediately of any breach of confidentiality or failure of safeguards, and any sanctions and remedial actions consequently imposed. DAC2 requires member states to ensure that any breach of security is also reported in turn to taxpayers when that breach is likely to adversely affect the protection of their personal data or privacy.

Part of the process for each jurisdiction adopting CRS includes a confidentiality assessment carried out by independent experts, to ensure that the jurisdictions have the necessary security and other arrangements to hold the data securely and avoid unlawful access. Clearly the UK and the jurisdictions it has specified to be reportable jurisdictions have been assessed as passing these assessments. No electronically held data is fully secure from cyber hacking or loss, but is HMRC – or any other tax authority deemed to meet the relevant data safeguards under the CRS, DAC2 and legal instruments – any more prone to cyber hacking or data loss than any other data controller, as the individual claimant here is apparently claiming?

DAC2 also requires that reporting financial institutions notify individual reportable persons that their data will be collected and transferred to tax authorities in sufficient time to enable such individual to exercise his data protection rights (e.g. to rectify incorrect data), which should be prior to reporting by the financial institution to its local tax authority. An arguable weakness within the UK legislation implementing CRS is that such notification can be made by UK reporting financial institutions in a one-off and general form, rather than a specific annual notification to individuals that are soon to be reported on. This means that an individual taxpayer may not know what precisely will be reported to whom by a financial institution in connection with that individual and the relevant financial account, and therefore could miss any opportunity to correct a mistake before the report is filed with HMRC and exchanged with other tax authorities under CRS. However, having specific prior notification obligations would impose significant additional administrative burdens on financial institutions.

It seems more likely that if the challenge made by the individual is successful, it would be on the grounds of a breach of the principle of proportionality in relation to the right to privacy rather than data protection

DAC2 also provides that information shall not be retained for longer than necessary to meet the objectives of the directive and in any case in accordance with domestic rules. Under UK rules, UK financial institutions effectively must retain CRS related information for six years. HMRC has a published general data retention policy that specifically references and seeks to comply with GDPR and the UK implementing legislation (the Data Protection Act 2018).

Conclusion

It seems more likely that if the challenge made by the individual is successful, it would be on the grounds of a breach of the principle of proportionality in relation to the right to privacy rather than data protection. It does, however, appear that CRS/DAC2 is not as soft a target as the Data Retention Directive. Were the challenge to succeed, the growing trend in recent years, stoked by public pressure in the wake of the financial crisis, for cross-border transparency measures that involve personal data may take a step back.

In the meantime, financial institutions should monitor the developments in relation to this and any further legal challenges in relation to CRS. Unless and until CRS/DAC2 is struck down altogether, financial institutions should continue to comply with their mandatory CRS due diligence and reporting obligations under applicable local implementing legislation. ■

For related reading visit www.taxjournal.com

- 20 questions on the common reporting standard (Hatice Ismail & Martin Shah, 2.6.16)