



12/05/2020

Government statement on cross-border information-sharing within corporate groups

To promote information-sharing within corporate groups, the Government is publishing this statement to advise regulated entities of when it is acceptable to share information. The Financial Action Task Force (FATF) sets international standards for anti-money laundering and counter-terrorist financing (AML/CTF) measures, and information-sharing is crucial to a number of its recommendations and immediate outcomes. FATF has issued guidance on private sector information-sharing, and in 2017 it made revisions to Interpretive Note to Recommendation 18 (INR.18). These underline the significance of private sector responsibilities in tackling ML/TF across borders and the value of cross-border information-sharing by the private sector as a key component of a well-functioning AML/CTF regime. Having reviewed the guidance set out by FATF as part of this process, the Government endorses it and affirms the value of well-governed information-sharing.

Information-sharing on a group-wide basis is a useful tool to prevent, recognise, investigate and report specific cases of ML/TF. It also enables global risk assessments, which corporate groups should undertake across all branches and majority-owned subsidiaries as the basis for their whole-group policies. Group-wide policies should result in better mitigation of risks, by enabling monitoring and sharing of information on customers, beneficial owners, account and transactions across the entire group, including across activities in different sectors. AML/CTF controls should be applied consistently. UK-based groups should ensure that their foreign operations meet UK requirements, to the extent that host countries' laws and regulations permit, as required by Regulation 20 of the Money Laundering Regulations.

By sharing information within a group, a regulated entity is better able to perform customer due diligence, more readily identify suspicious activity and file higher quality Suspicious Activity Reports (SARs) that take account of all of a customer's transactions with group members. This sharing may include information on which a SAR is based, the fact of a SAR having been filed, and a SAR itself, as permitted for credit and financial institutions by Section 333B of the Proceeds of Crime Act. It remains important to promptly file a SAR with the financial intelligence unit, regardless of any sharing. The FATF guidance sets out the kind of sharing that could be particularly useful.

Personal data from the UK should only be shared in a way that is consistent with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). Personal data that is shared between different organisations – even in the same corporate group – counts as a restricted transfer, if the transfer is sent or made accessible to a receiver to whom GDPR does not apply¹. These restrictions ensure that individuals' rights and freedoms for their personal data are protected, but there are tools available to facilitate transfers in a clear, safe and legal way. The Information Commissioner's Office (ICO) guidance on international transfers is a useful resource in relation to cross-border sharing of personal data and provides a more complete explanation of the following tools which exist to facilitate the transfer of personal data with full legal safeguards. The ICO also published a draft Data Sharing Code of Practice for public consultation in 2019. It provides practical guidance on how to share personal data. When finalised and laid in Parliament, this will be a statutory code which must be taken into account when sharing personal data between data controllers.

Notes:

Interpretive Note to Recommendation 18 is on page 80: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

¹ More detailed guidance about restricted transfers can be found on the [ICO website](#).