States of Guernsey
Income Tax

# Statement Concerning Data Protection for Financial Institutions submitting AEOI Data to the Director

Reporting Guernsey Financial Institutions (RGFIs) will be aware that they have an obligation to ensure that when sending data, which will then be forwarded to a third party, that their data is secure from the perspectives of how the data is handled by the Director, and also the IT protection against cyber security attacks in place with the Director.

This summary is intended to provide comfort to RGFIs that the information received by the Director is safeguarded appropriately. RGFIs may use this statement as part of their own internal risk assessments for the Director acting as a Third Party receiving the data, if desired.

Since entering into both the US-Guernsey (IGA) 'FATCA' and the Common Reporting Standard, Guernsey has been required to complete a detailed assessment of our data safeguarding measures and precautions for both AEOI Exchange Regimes.

A copy of the workbook completed for the US can be found here:

International Data Safeguards & Infrastructure Workbook

The questionnaire completed for the OECD is contained within the Standard for Automatic Exchange of Financial Account Information in Tax Matters as Annex 4 and can be accessed here:

Standard for Automatic Exchange of Financial Account Information in Tax Matters

In addition to completing these questionnaires, Guernsey was also subject to a site visit by the US IRS to look into the themes of the questionnaire in more detail. Similar site visits were undertaken on other Jurisdictions as a standard part of the assessment process.

The responses to both questionnaires contain sensitive information and as such, copies of these questionnaires, nor extracts of the answers given, are publically provided.

***Both the US IRS and also the OECDs assessments concluded that Guernsey was found to have adequate data safeguarding measures and infrastructure in place.***

States of Guernsey IT systems are also subject to periodic penetration testing, which it consistently passes. These include extensive tests undertaken on the IGOR portal including that of cyber security attacks on IGOR.

29 June 2016