

Anthony Smith
Chief Executive
Transport Focus

Fleetbank House, 2-6 Salisbury Square
London, EC4Y 8JX

w www.transportfocus.org.uk
t 0300 123 0860 f 020 7630 7355
direct 0300 123 0855
e jon.carter@transportfocus.org.uk

Date: 30 April 2019

Dear Anthony

SIRO's ANNUAL OPINION TO SUPPORT THE GOVERNANCE STATEMENT IN THE ANNUAL REPORT AND ACCOUNTS FOR 2018-19

I am required by HMG Security Policy Framework to provide you with an annual assessment on information risk to help inform the governance statement in the annual report and accounts.

I have consulted the several Information Asset Owners within Transport Focus and will additionally share this letter with the Audit, Risk Assurance and Remuneration Committee at its next meeting. I shall also place a copy of this letter on our website.

All Information Asset Owners keep their information assets under review during the year and provide a monthly statement to the Corporate Services Director in their budget holder declaration. It is planned however to make this important matter of assurance more bespoke during 2019-20.

The Information Strategy Group (ISG) meets quarterly, and reviews matters of information risk. This includes issues that we consider to be relevant and proportionate, based on any guidance from the Audit Risk Assurance and Remuneration Committee (ARARC). The ISG also conducts a quarterly risk assessment for each information asset which is then reviewed by the ARARC.

The year under review has been of the greatest significance in respect of information risk. The new General Data Protection Regulations (GDPR) took effect across the European Union during the year and has meant a considerable programme of mobilisation and delivery by ISG (and others) in general and by Michelle Jackson and me in particular. A considerable amount of work has been achieved, although some rewriting of the Information Risk Handbook remains outstanding. This work will be complete in 2019-20. The quarterly information risk assessment referred to above has been fundamentally overhauled to map data flows and be unequivocal in terms of the legal basis for processing personal data.



Significant time and energy has been spent on ensuring that our major databases – customer relationship systems for passengers and stakeholders, and our online panel – are, or will be soon, compliant and as risk free as it is possible to make them. This work will be complete during the first half of 2019-20.

A programme of GDPR workshops has been run across Transport Focus with the vast majority of staff attending. In addition, the majority of staff have completed mandatory training via the civil service online learning portal.

An internal audit in respect of GDPR preparedness took place during the year and reported a 'moderate' opinion. This was a good result. We are on track to complete the four 'high priority' actions from the report. One of these was, as you know, the appointment of a Data Protection Officer; I have been appointed to this role on a trial basis for 2019-20.

In respect of projects, data protection screens now replace privacy impact assessment screens in project workbooks, and no project is sent for approval unless the screen has been reviewed and authorised by me.

Michelle Jackson has been appointed Senior Information Asset Owner and will henceforth chair meetings of the ISG so that I am not conflicted in my role as Data Protection Officer.

The restructuring of the Manchester based contact team as a result of the introduction of the Rail Ombudsman is now largely complete. The smaller team will still retain its capacity for the first point of contact for individuals wishing to exercise their rights under the Freedom of Information Act 2000 or GDPR 2018.

I am also preparing my annual review on changes to risk levels as they apply to information assets, my annual consideration of how better use could be made of information assets, and an assessment of compliance against HMG Security Policy Framework mandatory measures. This work will be informed, as it is required to be, by the views of the various IAO's, and will be provided to the July ARARC meeting, if time permits.

Compliance with Freedom of Information Act requests during the year has been good, and all are reported to the quarterly ARARC meetings.

I am of the opinion that Transport Focus remains a low risk organisation, and that the actions we have taken as described above are relevant and proportionate to the risks we face. **There have been no reportable data incidents during the year.** I would therefore advise you that we should have no concern in claiming broad, proportionate, compliance with HMG Security Policy Framework (as it relates to information risk), and GDPR, within our annual governance statement.



I should like to add that those staff directly involved in the management of data take their responsibilities very seriously. I am very grateful to all of them for this – it would be impossible for me to do my job if this was not the case. This group not only includes our information asset owners, but others whose help in managing data in general, and preparing for GDPR in particular, has been amazing.

I am copying this letter to Shahid Mohammed.

Yours sincerely,

JON CARTER
Head of board and governance
Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO)