Regulatory Sandbox Final Report: Global Cyber Alliance

A summary of the Global Cyber Alliance's participation in the ICO's Regulatory Sandbox

Date: March 2022

ico.
Information Commissioner's Office

Contents

1. Introduction

1.1 The ICO introduced the Regulatory Sandbox ('Sandbox') service to support organisations that are developing products or services that use personal data in innovative and safe ways and where such products or services deliver a potential public benefit.

1.2 The ICO initially launched the Sandbox as a beta phase, for an initial group of participant organisations during 2019-2020. In August 2020, the ICO re-opened the Sandbox with a focus on projects involving one of two themes, children's privacy or data sharing in the areas of health, central government, finance, higher and further education or law enforcement. The ICO stated projects submitted should be at the cutting edge of innovation and may be operating in particularly challenging areas of data protection, where there is genuine uncertainty about what compliance looks like.

1.3 Organisations that were selected for participation in the Sandbox following its reopening have had the opportunity to engage with us, draw upon our expertise and receive our advice on mitigating risks and implementing 'data protection by design' into their products or services, whilst ensuring appropriate protections and safeguards are in place. The Global Cyber Alliance (GCA) was one of the candidates selected for participation in the Sandbox after it re-opened.

1.4 The GCA is a non-profit organisation with a singular purpose: to make the Internet a safer place by reducing cyber risk. The organisation builds and provides a range of programs, tools and partnerships to sustain a trustworthy internet to enable social and economic progress for all. One of the solutions developed by the GCA is their Domain Trust product which is described in section 3 of this report.

1.5 Due to potential data protection risks that could be associated with possible, future evolutions of this project, the GCA applied to enter the ICO's Sandbox. The GCA was accepted into the Sandbox on 23 November 2020 and a Senior Case Officer was appointed. The Senior Case Officer conducted a scoping call with the original GCA representative on 3 December 2020 to gain an insight into the organisation and begin formulating the objectives and tasks of the GCA's Sandbox plan.

1.6 Following the call in December 2020, the ICO and the GCA agreed the following objectives for the GCA's Sandbox engagement:

- **Objective 1:** The ICO and the GCA will evaluate integrating ICO investigations data, regarding known or suspected malicious domains, into the Domain Trust platform.
- **Objective 2:** The ICO will provide steers to the GCA around the processing of personal data for consideration in the evolution of the Domain Trust platform, with particular consideration given to Part 3 of the Data Protection Act 2018 (DPA18) (ie law enforcement processing).
- **Objective 3:** The ICO and the GCA will work together to evaluate other key data protection considerations (in relation to the UK GDPR) surrounding the Domain Trust platform.

1.7 The content of the Sandbox plan was agreed by Andy Bates, the then Executive Director for the UK, Middle East and India of the GCA, and the ICO on 26 January 2021.

1.8 In October 2021, the GCA and the ICO completed the last piece of work detailed in the GCA's Sandbox plan, bringing the GCA's participation in the ICO's Sandbox to an end.

1.9 Also in October 2021, the GCA appointed Dan Owen as Product Owner to oversee all aspects of the Domain Trust product, including the responsibilities of coordinating with the ICO on the Regulatory Sandbox final report and to be the GCA's operational point of contact for all issues related to Domain Trust in the future.

1.10 On 8 December 2021, the GCA notified the ICO that the possible, future evolution of the Domain Trust project was no longer being considered and would not be implemented. This included the scope and content of all of the previously agreed objectives. However, understanding the substantial work that the ICO committed to this Sandbox effort, the GCA agreed to move forward with this final report so that the ICO's assessments of data protection risks of these particular types would be documented and made available to the public.

1.11 Effective January 2022, the GCA's Chief Legal Officer, Mary Kavaney, is the appointed primary representative to all regulators and will be the GCA's primary leadership point of contact to the ICO for all other matters beyond the scope of Domain Trust operations.

2. Executive summary

2.1 As detailed above, the GCA's stated aim in providing its products and services is to make the internet a safer place by reducing cyber risk. The Domain Trust platform does this by providing domain Registrars, Registries and other parties with some of the information needed to determine which domains should be blocked or unregistered, depending on the operational role of the party. The GCA entered the ICO's Sandbox with the stated aim of ensuring that the Domain Trust platform achieves its goal in a way that respects individuals' rights and is compliant with UK data protection legislation.

2.2 Since January 2021, the GCA have worked with the ICO to assess the possible data protection risks associated with the Domain Trust platform as it currently processes data. The GCA and ICO also sought to identify risks associated with new forms of processing that Domain Trust had previously considered undertaking in the future but has since set aside.

2.3 In line with the objectives outlined in the GCA's original Sandbox plan, the ICO and the GCA have worked together to achieve the following objectives:

- **Objective 1: The ICO and the GCA will evaluate integrating ICO investigations data, regarding known or suspected malicious domains, into the Domain Trust platform.**

  While working on this objective, the Sandbox team have drawn together opinions and views from across the ICO to assess whether the ICO has the power to share some of the data gathered during the ICO's investigatory activities to contribute to the work carried out by the GCA via the Domain Trust platform.

The ICO first considered whether this sharing would be considered a disclosure of personal data and decided that, on balance, in some circumstances the disclosure of domain names could include personal data (ie any information relating to an identified or identifiable natural person or 'data subject'). As such, the GCA was advised to ensure that they could comply with applicable data protection requirements in relation to this processing and that the steps they were taking to comply were proportionate to the processing activity itself.

After careful consideration it was decided that sharing and integration of ICO investigations data regarding known or suspected malicious domains, into the Domain Trust platform, was not feasible at this time. However, the ICO is in the process of updating their breach reporting forms with a link to the National Cyber Security Centre (NCSC) so that those reporting a relevant breach can inform the NCSC directly.

Objective 2: The ICO will provide steers to the GCA around the processing of personal data for consideration in the evolution of the Domain Trust platform, with particular consideration given to Part 3 of the DPA18 (ie Law enforcement processing).

The ICO has provided the GCA with steers under the following key headings during their time in the Sandbox:

- **Criminal offence data considerations**

  During the GCA's Sandbox participation, the ICO provided advice around the considerations the GCA would need to take if a decision was made to process potential criminal offence data in the future with the Domain Trust product. These steers covered topics such as:

  - Is the data provided to the GCA from contributing parties data that is processed for law enforcement purposes as defined in Section 31 of the DPA18?
  - Would the ICO have any authorisation in law to contribute data to Domain Trust?

- The legalities of requesting data about known or suspected malicious domains from domain Registrars, Registries and other parties, and sharing this data with other Registrars, Registries and other parties, to assess the threat associated with an individual's entire portfolio of domains rather than just a singular domain, as a means to expand the accuracy and comprehensiveness of such data within the Domain Trust product.

- **Lawful basis considerations**

  During the GCA's Sandbox participation, the ICO provided advice around lawful basis for the following potential processing activities associated with the Domain Trust product[1]:

  - The transfer of global law enforcement organisations' domain-related data, which potentially contains personal data, to and from the GCA.
  - The transfer of global Registrars', Registries' and other parties' domain-related data to and from the GCA, which potentially contains personal data.
  - The further transfer of Domain Trust data by and between Registrars, Registries and other parties.

Objective 3: The ICO and the GCA will work together to evaluate some other key data protection considerations (in relation to the UK GDPR) surrounding the Domain Trust platform.

[1] Please note it is not appropriate for the ICO as a regulator to determine the lawful basis upon which a contributor should rely when processing personal data; however, as it is likely the GCA and Registrars, Registries and other parties will be acting as independent contributors for separate aspects of the processing activities surrounding Domain Trust, the ICO have provided some suggestions below that each contributor will need to consider before processing this data.

During the GCA's Sandbox participation, the ICO and the GCA worked together on several key pieces of documentation to ensure that possible data protection-based risks associated with the Domain Trust product were considered and mitigated. These documents included:

- A data protection impact assessment (DPIA)
- A legitimate interests assessment (LIA)
- The GCA's data protection policy

3. Product description

3.1 The GCA's Domain Trust product collects data from multiple sources on known or suspected malicious domains that can be passed to Registrars, Registries and other parties that administer and manage these domains and the access to them, so that these parties can intervene in some way, by blocking them, temporarily suspending the domain or taking the domain down altogether. Prior to their participation in the Sandbox, the GCA had designed this process to avoid processing data that is strictly personal data (ie only domain names are collected and shared).

3.2 The first objective of the GCA's original Sandbox plan focused on integrating some ICO investigations data about known or suspected malicious domains into the Domain Trust platform. This is referred to as strand one processing and was envisaged to work in the following way[2]:

1. The ICO, through reporting or monitoring, becomes aware of known or suspected malicious activity associated with a particular domain and may collect multiple data types associated with that domain.

2. Domain Trust assigns the ICO an assurance rating based on the GCA's internal taxonomy and the types of data normally provided by the ICO.

3. The ICO shares the name of the domain(s) with Domain Trust via an API key.

4. The ICO contributes names of domains to Domain Trust and categorises submissions based on the level of certainty that a given domain is known or suspected to be malicious.

5. The ICO identifies the date and time they first made a record of the domain in their system and the GCA issues a timestamp for when a particular domain is submitted to the Domain Trust platform.

6. Domain Trust makes these contributed domain names available to all global partners that have signed a memorandum of agreement and have agreed to the GCA's terms of service.

7. Registrars, Registries and other parties may access Domain Trust to review all domains contributed by all global partners and are able to see taxonomy categorisations for each domain contributed.

8. Registrars, Registries and other parties may then use this information in determinations of whether to block or take down individual known or suspected malicious domains, preventing them from being used for further criminal activity.

3.3 The second strand of processing activities, objectives two and three of the original Sandbox plan, explored the data protection implications of GCA utilising more personal data in the Domain Trust platform. This would allow the GCA to gain further intelligence on the domains utilised by cyber criminals to commit crimes, if such an evolution were to occur in the future.

3.4 This potential second strand of processing activities for GCA[3] involves sharing personal data which is likely to constitute criminal offence data between different parties. This would include both domestic and international data sharing.

3.5 The personal data that Domain Trust had considered processing in the future could have included the registration information that Domain Registrants have provided during the registration process. For example, those who have registered or purchased a domain from a Domain Registrar. GCA is no longer considering this use.

4. Key data protection considerations

4.1 The GCA's participation in the Sandbox focused on considering all the key data protection considerations associated with the possibility of evolving the Domain Trust product to incorporate additional personal data. In order to consider these issues the ICO and the GCA agreed upon the objectives in the GCA's original Sandbox Plan, the details of which are outlined below.

Objective 1: The ICO and the GCA will evaluate integrating some ICO investigations data, regarding known or suspected malicious domains, into the Domain Trust platform.

4.2 In order to complete the GCA's first objective, the ICO facilitated a workshop in January 2021 with key members of ICO staff to discuss the potential security and data protection implications of inputting information on known or suspected malicious domains identified in data breach investigations into the Domain Trust platform. During the workshop, the ICO and the GCA agreed upon actions to progress this work stream that focused on assessing whether the ICO already collects the domain-related data in a format which can be used for Domain Trust's purposes.

[3] Please note that the GCA were exploring this as a possibility and has no current or future plans to request, collect and process personal data associated with known or suspected malicious domains, but has sought the ICO's view on data protection considerations associated with processing additional personal data, if such an evolution of the platform were to occur in the future.

4.3 The ICO also considered whether the data processed was personal data at all. The GCA informed the ICO that the information processed by Domain Trust includes a disclosure of the known or suspected malicious domain (eg domainname.org), the date and time a record of the domain is created by the contributor and a timestamp with the date and time the domain is submitted to the Domain Trust platform. The ICO informed the GCA that it appears likely that disclosures of this nature would not involve processing any personal data; however, the ICO asserted that there is a small risk that the information disclosed may contain some elements of personal data (eg if a suspect domain includes an individual's name such as JoeBloggs3.org).

4.4 Existing ICO guidance on "What is personal data?" states:

> "information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data."

4.5 ICO guidance further states that personal data is information that relates to an identified or identifiable individual and that, even if an individual is identified or identifiable, directly or indirectly from the data being processed, it is not personal data unless it 'relates to' the individual. When considering whether or not information 'relates to' an individual, contributing bodies (in this scenario the ICO) will need to take into account several factors including the content of the information, the purpose or purposes for which the GCA are processing it and the likely impact or effect of that processing on the individual. In order to evidence that they have fully considered whether or not the domain-related data processed is personal data, the GCA should also, potentially as part of their DPIA, complete a 'relates to' test where they consider:

- the content of the information (eg a domain name containing a personal name, if the name relates to an individual);
- the purpose or purposes for which they are processing the data; and,
- the likely impact or effect of that processing on the individual (eg would the data be used, or likely to be used, to learn, evaluate, treat in a certain way, make a decision about, or influence the status or behaviour of an individual).

4.6 It is logical to assume that in some circumstances reported domains may include elements of personal data . For example, in a situation where a cybercriminal is spoofing the legitimate website of a sole trader in order to divert payments intended for that sole trader. It is likely that the ICO would view this sharing as a potential transfer of personal data. As such, the GCA is advised to ensure they take steps to comply with applicable data protection legislation to reflect the fact that they may be engaging in data processing in this way.

4.7 In addition to the lawfulness of the sharing, the ICO also had to consider whether the information being requested was held in such a format that could be readily integrated into the Domain Trust platform.

4.8 After careful consideration it was decided that sharing and integration of ICO investigations data regarding known or suspected malicious domains, into the Domain Trust platform, was not feasible. However, the ICO has now updated their breach reporting forms with a link to the NCSC so that those reporting a relevant breach can inform the NCSC directly.

Objective 2: The ICO will provide steers to the GCA around the processing of personal data for consideration in the evolution of the Domain Trust platform, with particular consideration given to Part 3 of the DPA18 (ie Law enforcement processing).

Criminal offence data considerations

4.9 If, in the future, global law enforcement organisations and supervisory authorities (including, but not limited to, those listed in the DPA18) become contributing parties to the Domain Trust platform, it is necessary to determine if the sharing of personal data with the GCA would have a suitable authorisation in law. The Sandbox team provided steers to the GCA around this point in respect of both strands of their processing activities, should the GCA ever process this data in the future.

4.10 With regard to the GCA's first strand of processing activities (ie possibly receiving personal data provided to them by range of organisations including data held by the ICO) the ICO first considered whether or not these organisations and the GCA are processing the data for law enforcement purposes, as defined in Section 31 of the DPA18 as processing for[4]:

> 'The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

4.11 Given the GCA is not a competent authority as listed in Schedule 7 of the DPA18, it is likely that some organisations involved (including the ICO if they were to provide this) in contributing data to the Domain Trust platform, would be transferring data within the scope of Part 3 of the DPA18 to an organisation processing that data under UK GDPR Part 2. In order to ensure that this transfer is compliant with the DPA18, the GCA should ensure that these contributing bodies have determined whether or not they have suitable authorisation by law to disclose this information, as per Section 36(4) of the DPA18.

4.12 The Sandbox team also considered whether the ICO would have suitable authorisation by law to transfer their own data on known or suspected malicious domains into Domain Trust as part of their considerations around objective one and the GCA's Sandbox plan. In order to consider whether the ICO had suitable authorisation by law to disclose the information the ICO considered Section 132 of the DPA18 which states that:

> 'A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—
>
> (a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the

[4] It was concluded that it was not feasible for the ICO to share this data.

Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.'

4.13 As the data the GCA processes may be obtained by the ICO inadvertently during the course of discharging its investigative functions when investigating cyber based data breaches, the ICO must ensure any such disclosures are 'authorised by law'.

4.14 The GCA originally wished to explore a possible second strand of processing, whereby Registrars, Registries and other parties might transfer to Domain Trust personal data including registration information for individuals who have registered known or suspected malicious domains. The ICO advised the GCA that as contributing parties may be sharing this personal data with the GCA via Domain Trust they would need to ensure there is a suitable lawful basis in place for these transfers of data. The ICO advised that Registrars, Registries and other parties may be able to rely on legitimate interests as their lawful basis for processing, although this would depend on the context in which each party was sharing the personal data and is ultimately an assessment that can only be made by those parties.

4.15 As the personal data involved in these types of transfers may relate to suspected criminal offences, and when neither the contributing party nor the GCA is a competent authority[5] the contributing party requires an appropriate basis in law to undertake the transfer (as defined in Section 10(5) of the DPA18). This means that such transfers of personal data could be undertaken, provided the contributing party meets a condition in Part 1, 2 or 3 of Schedule 1 of the DPA18. It is possible that the contributing party would be able to use one of the substantial public interest conditions listed in Part 2 of Schedule 1 (such as the prevention and detection of unlawful acts) to undertake the transfer, but this is ultimately an assessment that

[5] It should be noted that even if the contributing party is a competent authority it still needs to identify a lawful basis for processing and schedule condition if it's criminal offence data, as well as identifying whether the new purpose is compatible with the original purpose and whether the sharing is authorised by law.

only the contributing party can make. The ICO also recommends the GCA ensure, to the extent possible and as part of their due diligence process, that each contributing party have their own appropriate policies in place and documented for such transfers (as required by DPA18, Schedule 1 Part 2(5)) before any such transfers take place.

4.16 Similarly, in order to undertake further possible sharing of the data provided by contributing parties, the GCA would need to select their own substantial public interest condition and create their own appropriate policy document in accordance with the requirements of DPA18, Schedule 1 Part 4.

Lawful basis

4.17 If such an evolution of the Domain Trust platform were to occur in the future where additional data beyond domain names, such as criminal offence data is processed, there is a possibility such additional data could be personal data. The ICO advised the GCA that it would not be appropriate for the ICO as a regulator to determine upon which lawful basis a controller should rely on when processing personal data. However, as it is likely the GCA, Registrars, Registries and other parties will be acting as independent controllers for separate aspects of the processing activities surrounding Domain Trust, the ICO have provided some suggestions below which each controller will need to consider before processing this type of data.

4.18 If GCA decided to take strand two of processing forward, the first processing activity that may take place is the transfer of personal data from law enforcement bodies and regulators to the GCA. As discussed above, some organisations will be transferring personal data already processed under Part 3 of the DPA18 to the GCA, which will mean this processing will take place under the framework provided by Part 2 of the DPA18. It is likely that these organisations may be able to rely on legitimate interests (GDPR Article 6(1)(F)) as the basis for transferring data to the GCA, and if it falls under part 4 Data

Protection Act 2018 criminal offence data, a schedule condition will also need to be identified, but obviously each party will need to make this assessment in the context of each organisation's own respective activities[6].

In respect of the first processing activity, it would be up to each individual contributing party to determine if they should transfer personal data and it would not be appropriate for the ICO to suggest that any party transfer personal data in the first place, nor specify the lawful basis upon which they should rely on in relation to this data transfer. It does, however, appear likely that any transfer of personal data would be considered lawful if the contributing parties identify a suitable lawful basis for processing, under Article 6 of the UK GDPR. The ICO also recommends each contributing party ensure that they are also complying with the relevant data protection legislation in the territory in which they operate.

4.19 The ICO advised that the GCA will also need to consider the basis for processing upon which they rely if, in the future, they might begin transferring personal data on suspect domains provided by law enforcement to Registrars, Registries and other parties. It is possible that the GCA could rely on legitimate interests. As discussed above, because the data may be criminal offence data, the GCA would also need to consider Article 10 of the UK GDPR to ensure they can satisfy a valid condition under which they can transfer any criminal offence data they may have obtained. DPA18 Part 2 Section 10(1)(B) 'substantial public interest' may be an appropriate condition for the GCA's purposes. The exact public interest pursued would be the prevention and detection of unlawful actions DPA18 Schedule 1(10). The GCA were advised that as they are not a competent authority and would not be processing this personal data on the behalf of a competent authority, or disclosing this data to a competent authority, they would need to have an appropriate policy document in place (as detailed in DPA18, Schedule 1, Part 4).

[6] Please note – any competent authority will also need to ensure that their sharing or transfer of data is authorised by law as well as having a suitable basis for processing. Further information on sharing and reusing personal data for non-law enforcement purposes can be found in ICO's guidance.

For the second part of the potential processing activity, where the GCA may be sharing personal data obtained from contributing parties with other Registrars, Registries and other parties, it is likely that the GCA would need to identify their separate legitimate interests for undertaking this further processing activity.

4.20 In some instances, these transfers could potentially be made to Registrars, Registries and other parties located in countries outside of the UK. In such circumstances, where the GCA might transfer personal data outside of the European Economic Area (EEA), this is likely to involve an international transfer that needs to comply with the requirements of Article 46 of the GDPR. For the GCA's purposes it appears likely that GDPR Article 46(2)(D) regarding the use of standard contractual clauses may be the most appropriate mechanism to use; however, this decision ultimately rests with the GCA and they should consider whether any of the other Article 42(2) conditions are more suitable for their purposes[7].

Objective 3: The ICO and the GCA will work together to evaluate some other key data protection considerations (in relation to the UK GDPR) surrounding the Domain Trust platform.

During the GCA's Sandbox participation the ICO and the GCA worked together on several key pieces of documentation to ensure that possible data protection-based risks associated with the Domain Trust product were considered and mitigated. These documents included:

- **A Data protection impact assessment (DPIA) –** In completing a DPIA, the GCA primarily sought to assess whether their originally proposed processing activities were proportionate to their aim of reducing the number of known or suspected malicious domains on the internet. For strand one of processing activities this included balancing the minimal amount of processing of personal data against the potential to cause real harm to individuals and businesses if they were to make ICO-contributed data available to Registrars, Registries and other parties that might lead to legitimate websites being taken down. If the GCA moves toward implementing any 'strand two' processing, the ICO recommends that they

[7] It should be noted that transfers to Registries and Registrars in the EU will not need to use standard contractual clauses as these organisations have adequacy findings, as will other non-EU countries that have adequacy findings.

create a suitable DPIA to fully consider the risks associated with such processing while they develop an appropriate technical framework around the sharing and processing to ensure that data subjects' rights are considered and protected before the processing commences.

- **A legitimate interests assessment (LIA) –** As the GCA may look to rely on legitimate interests as their lawful basis for potential future processing of data associated with the Domain Trust platform, they completed a LIA and balancing test in order, among other things, to assess the proportionality of such processing of personal data in the context of their goal of preventing cybercrime.

- **GCA's data privacy notice –** Due to the nature of the Domain Trust platform, it is unlikely that data subjects would be aware that GCA may process their personal data via Domain Trust, if such an evolution of the platform were to occur in the future. In order to ensure that data subjects are informed about how Domain Trust may process their personal data and what data they may process, the ICO has provided the GCA with comments and suggestions on their public facing privacy notice, which is on the GCA's website. It is hoped that the GCA will use these comments and feedback to continue to iterate and improve on this policy so data subjects can be fully informed about how the GCA may process their personal data.

4.21 Over the course of the GCA's Sandbox participation, the ICO has reviewed several iterations of these documents and has provided extensive notes, comments, and suggested edits for the GCA to consider. It is recommended that the GCA will use the ICO's feedback to continue to improve these documents and assess any new risks that may come to light in relation to the Domain Trust product.

5. Ending statement

5.1 The GCA's participation in the ICO's Sandbox has given the ICO the opportunity to contribute towards and gain insight into how complex, international data sharing initiatives can assist organisations attempting to reduce instances of cybercrime and ultimately make the internet a safer environment for its users.

5.2 The GCA has sought to demonstrate its commitment to making use of innovative technology in compliance with UK data protection legislation, in relation to the above objectives, as it deploys the Domain Trust platform to further its goal of making the internet a safer space for all its users. Through this work, the ICO recognises that there are likely to be several challenges faced by organisations undertaking similarly complex data sharing initiatives, which include ensuring that:

- adequate and proportionate fair processing of information is provided to data subjects to ensure they are informed about an organisation's processing activities;
- suitable due diligence is carried out on the recipients of personal data to ensure it is processed consistently (ie that these parties have a compatible purpose for processing, that common security standards are in place);
- compliant mechanisms are in place if transferring and sharing data internationally both in the EEA and beyond; and,
- a suitable, lawful basis for sharing and further processing of personal data has been identified by the recipient of the personal data prior to any sharing of personal data.

5.3 Based on the information we have reviewed as part of the GCA's Sandbox participation and, solely in respect of the originally considered first strand of the Domain Trust processing to integrate future ICO data[8], it appears likely that the GCA has complied with its obligations as a controller under the UK data protection legislation. Whilst the GCA is no longer considering and will not be implementing the incorporation of personal data as described in the scope of the three objectives for this Sandbox engagement, the steers and relevant guidance will be useful for the GCA moving forward. The GCA should continue to follow the steers provided and relevant ICO guidance with the same diligence and transparency it has demonstrated during its participation in the Sandbox, if the GCA moves forward with any possible future evolution of the Domain Trust product that may incorporate personal data.

5.4 The GCA’s participation in the ICO Regulatory Sandbox demonstrates the ICO’s role as a trusted regulator in its support for stakeholders who ensure that information rights are recognised, respected and designed into the fabric of data sharing projects, demonstrating that UK data protection legislation is not a barrier to innovation.