GDPR Compliance Programme: Proposed personal data mapping exercise

Purpose of this briefing note

To outline a proposed personal data mapping exercise which forms a key element of TfL's GDPR Compliance Programme.

Background and context

From May 2018, TfL and its subsidiaries will be required by law to create and maintain comprehensive records of any data processing activities involving personal information across all business areas, services and operations.

Section 2 of the ICO's guidance document "Preparing for the General Data Protection Regulation – 12 steps to take now", published in 2016, states:

" *You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit, across the organisation, or within particular business areas. The GDPR updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.*"

Section 6 goes on to add that:

" *You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it…Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your legal basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your legal basis for processing. You will also have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. The legal bases in the GDPR are broadly the same as those in the DPA so it should be possible to look at the various types of data processing you carry out and to identify your legal basis for doing so. Again, you should document this in order to help you comply with the GDPR's 'accountability' requirements.*"

Personal data mapping activities have been the focus of considerable comment and discussion amongst data protection lawyers and practitioners. Short articles from two specialist journals are included at Appendix 1 and Appendix 2 of this briefing note.

TfL does not currently hold any form of information asset register or personal data inventory which could provide the necessary level of detail to support TfL's GDPR Compliance Programme, or satisfy the new record keeping requirements contained in Article 30 Recital and 82 of the GDPR.

Whilst there are some lists of data repositories which contain personal data, none of these encompass all of the TfL business areas involved in the processing of personal data; nor do they include details of personal data types, sources (and associated privacy notices), processors (and associated data processor agreements), sub-processors, onward disclosures (and associated information sharing agreements), or the legal basis for processing (ie consent, legitimate interest, performance of a contract, express statutory powers, etc).

Consequently, some form of personal data mapping exercise focussed on TfL, its subsidiaries (and a number of outsourced operations delivered by external service providers) is recommended and would ideally be completed by the end of August 2017. This data mapping exercise would be limited to establishing the current nature, scale and distribution of TfL's personal data holdings and associated data processing activities.

The target completion date of 31 August 2017 would provide an eight month period during which the Privacy and Data Protection Team would be able to:

1. perform a gap analysis and identify "high risk" data processing activities (including any profiling or surveillance of customers and employees); and
2. put in place any urgent remedial actions (eg Data Protection Impact Assessments; new/amended privacy notices, information sharing agreements and data processor agreements; personal data cleansing and deletion).

The outputs from the personal data mapping exercise would need to be collated and captured in some form of central register or database. This repository will form an essential component of TfL's wider GDPR Compliance Programme and will need to be made available for inspection by the relevant Supervisory Authority (ie the information Commissioner's Office) on request.

In terms of future maintenance of the personal data maps created a result of this exercise, TfL's instance of TRUSTe Assessment Manager (a cloud based online tool used to conduct Data Protection Impact Assessments and create other bespoke interactive compliance questionnaires) would be used on an ongoing basis to capture the details of required updates/amendments.

That process would be co-ordinated by the Privacy and Data Protection Team, with input from the Information and Records Management (IRM) Team, Personal Information

Custodians (circa 60 senior managers with responsibility for systems and processes which are used to process personal data) and individual business areas.

NCC Proposal

On 8 February 2017 NCC were invited via TfL's Commercial function to submit a proposal for a personal data mapping exercise under Lot 1 of TfL framework agreement ITC11524. Using this particular framework agreement (also used by both Internal Audit and Technology & Data for the delivery of outsourced PCI DSS and cyber security services) means that a potentially lengthy procurement process is not required and work can be started within a relatively short timeframe.

NCC's response is attached to this document as Appendix 3. The total cost quoted is [redacted] (exclusive of VAT). The production of associated data flow diagrams would cost an additional [redacted] per diagram. A total of between 10 and 15 diagrams would be desirable, each covering a specific processing activity (eg Oyster online registration and account management; and Congestion Charge Auto Pay account creation/management).

The proposal satisfactorily addresses all of the requirements specified in the original request and demonstrates a good understanding of the records keeping and accountability requirements of the GDPR. It was made clear to NCC that their role in the data mapping exercise would not encompass non-personal data discovery, or the development and implementation of specific remedial actions or solutions to address instances of non-compliance with data protection legislation or TfL policies/ procedures.

NCCs' knowledge of TfL and its wholly owned subsidiaries (acquired as a consequence of the extensive PCI DSS and cyber security assurance work that they have been carrying out across the group for a number of years), should ensure the timely and efficient completion of the personal data mapping exercise.

In addition, we would expect NCC to leverage some existing TfL resources as part of this exercise, in particular our instance of TRUSTe Assessment Manager, our internal network of Personal Information Custodians and the knowledge/insights of members of the Privacy and Data Protection Team and IRM Team.

In terms of funding the personal data mapping exercise, three possible options have been identified and are summarised below.

Funding option 1 – General Counsel funding

The first and perhaps most straightforward option, would be for General Counsel (the business area ultimately responsible for privacy and data protection compliance) to fund the cost of the exercise from any underspend identified within its 2016-17 budget.

Funding option 2 – Voluntary contributions from the business

If General Counsel is unable to identify adequate resources, a second option would be for the Privacy and Data Protection Team to approach those business areas which process the largest volumes of personal data and request an appropriate contribution towards the cost of the personal data mapping exercise. In the event that this is the favoured funding approach, a suggested breakdown of contributions is included below:

1. **33%** Technology & Data
2. **20%** Surface Service Operations
3. **12%** Human Resources
4. **10%** Enforcement and On-Street Operations
5. **5%** Marketing
6. **5%** Road Space Management
7. **5%** Bus Operations
8. **2%** LU Network Security & Policing
9. **2%** LU Revenue Control
10. **2%** Occupational Health
11. **2%** Pensions
12. **2%** Group Property & Facilities

Although potentially a complex and time consuming approach, partly because of its voluntary nature, there is a precedent (albeit on a smaller scale). In 2015 a customer privacy research exercise was funded with contributions from General Counsel and six other business areas.

Funding option 3 – ExCo approved 'top-slice' funding

The third option would be for General Counsel to ask the Commissioner and other members of ExCo to discuss and agree the most appropriate division/sources of funding for the cost of the exercise; and for that decision to be communicated to the relevant business areas and actioned.

Next steps

Agreement as to whether:

1. TfL should proceed with a personal data mapping exercise as part of its GDPR Compliance Programme;
2. the proposal from NCC satisfies all of the relevant criteria; and if so, which of the three funding options would be the most appropriate to pursue.

James Alexander
Head of Privacy and Data Protection

17 March 2017

APPENDIX 1

APPENDIX 2

APPENDIX 3

Data Discovery

GDPR Compliance Programme - Personal Data Mapping Exercise

Framework No: ICT11524 – Lot 1

Request Form Number: LRF014

Proposal for Transport for London

February 2017

The digital world is becoming ever more dangerous. With cyber-attacks on the increase and more companies choosing to drive their digital strategy forward, some of your most valuable assets are on display for the world to see.

NCC Group can help. With a world-class team of experts, supported by leading technology and processes, we will work with you to make sure your data is protected. We know how hackers think and act, and will share this information with you to make sure you keep your freedom from doubt.

Table of Contents

For more information, please contact:

Name: [redacted]

Email: [redacted]

Phone: [redacted]

Proposal Ref: P68030

Version 0.1

Executive summary

Identifying and mapping your critical data is key to your business operations, to your clients and service users

Understanding your needs

The General Data Protection Regulation (GDPR) will come into force in May 2018. As a result of this new legislation, TfL will become subject to a new legal obligation to create and maintain comprehensive records of its data processing activities involving personal information across all business areas, services and operations.

In addition, to fully assess privacy and compliance risks under the new law, data controllers will need to be able to answer the following questions about their processing of personal data: -

- What personal data is being collected?
- How is that personal data being created / captured / collected?
- Why is that personal data being created / captured / collected?
- How is that personal data being used?
- Where is that personal data being stored?
- How is that personal data being secured?
- Who has access to that personal data?
- Who is that personal data being shared with?
- How long is that personal data being retained?
- How is that personal data being deleted / destroyed?

As a result, TfL is considering commissioning a personal data mapping exercise, focusing on TfL, its operating subsidiaries (including London Underground) and a number of outsourced operations delivered by external service providers (including Cubic Transportation Systems Ltd, Capita plc, NSL, Dawley Services Ltd, Marston Group, Independent Transport Associated Limited, Journeycall Ltd and Novacroft Ltd).

As a large organisation with millions of customers, tens of thousands of employees, hundreds of systems and reporting tools, dozens of external data processors and data types – it is expected to be a complex and challenging exercise.

Therefore, NCC Group has been approached to provide a detailed proposal to address TfL's requirements, which will describe the following: - the intended methodology, the resources we will need to deploy, the anticipated timescales, the suggested project governance and reporting arrangements, and the associated costs for TfL.

We deliver a pragmatic and accessible view of your sensitive and critical data assets. This allows you to target risk assessment activity and focus your resources.

Key Objectives

The key objectives for this engagement are as follows: -

- That the personal data mapping exercise will form an essential component of TfL's GDPR Compliance Programme and be treated as a distinct work stream within that wider programme.
- The answers to the questions outlined in the Executive Summary above will need to be collated and captured in some form of central register or database which can subsequently be maintained and updated independently by TfL.
  - In addition, the exercise should also take into account the relevant provisions of the ICO GDPR Guidance (Accountability and Governance section) – "Recital 82" and "Article 30" – Records of Processing Activities". These are included within the main body of the proposal for reference.
- The data mapping exercise will also need to highlight high risk data processing activities (including any profiling or surveillance of customers and employees) based on a pre-determined risk matrix to be agreed with TfL, so that data protection impact assessments can subsequently be carried out by TfL, once the data mapping exercise has been completed.
- Leverage existing TfL resources as part of this exercise, in particular: -
  - TfL's TRUSTe Assessment Manager – a cloud-based online tool to conduct Data Protection Impact Assessments and create other bespoke interactive compliance questionnaires.
  - The internal network of Personal Information Custodians – 60 senior managers with responsibility for systems and processes which are used to process personal data.
  - The knowledge and insights of members of TfL's Privacy and Data Protection Team – 5 individuals who work across TfL on matters relating to privacy and data protection compliance.
- That the data mapping exercise is limited to establishing the current scale and distribution of TfL's personal data holdings and the associated data processing activities. It is not intended to extend to non-personal data discovery, or the development and implementation of remedial actions or solutions to address instances of non-compliance with data protection legislation or TfL policies / procedures.

With this in mind, NCC Group is capable of supporting your key objectives by providing the following assistance: -

- Using questionnaires and by conducting interviews with the 60 Personal Information Custodians, categorise, identify and locate critical, sensitive data assets

- Map the data assets by building a data asset inventory (in MS Excel workbook)
- Provide an accompanying executive summary report which includes:
  - Description of approach taken.
  - Executive Summary of Findings.
  - Data categorisation and sub categorisation and data types.
  - Identification of Personally Identifiable Information (PII) as well as other critical business information (where applicable).
  - Storage and processing locations for data in electronic and physical hard copy format.

NCC Group has successfully engaged with a number of large organisations on a range of data mapping and GDPR projects. These projects have involved organisations experiencing similar challenges to those currently facing TfL, and our consultants have considerable experience in assisting them with addressing these challenges.

The key attributes we can offer are:

- Ongoing experience of working with high-profile multinational blue-chip organisations in mapping data across complex multinational operations.
- Providing trusted advisor recommendations on policies, procedures, systems and technologies to assist you with follow on activities.
- Guaranteed independence from all suppliers of technology and security products, ensuring impartial advice and guidance at all times.
- Proven experience, covering more than 250 years of IT security experience across our team.
- Proven quality, as demonstrated by our ISO 27001 certification. We are one of the few consultancy firms who carry the ISO 27001 accreditation. This means that not only do we practise what we preach, but we also have invaluable experience of what is required to bring an organisation into line with an internationally accepted security standard, from the point of view of the organisation, rather than merely as advisors.

Understanding your challenges

Why are your data assets at risk?

Risks

- Cyber attacks on business systems are increasing year on year.
- Insider threat is real, where staff either steal, or accidentally expose data.
- Criminals target businesses and employees through employing sophisticated techniques that exploit behaviour leading to data loss.
- The digital landscape is changing due to outsourcing, use of cloud solutions and suppliers accessing data and its repositories.
- The value of sensitive data (e.g. critical operation or personally identifiable data) is increasing and readily sold on the internet to criminal elements.

The Data Asset Problem

Key Issues

- Organisations can no longer understand data value or where it is stored. Data sensitivity and criticality is not identified or understood. Some data is highly sensitive (PII) and should be treated security by law (EU GDPR).
- Highly sensitive data can appear in electronic form in local storage, email, shared system drives, application and database servers, portable storage devices, and in several cases, also in hardcopy format.
- Data usage and sharing is widespread and can proliferate quickly and easily across multiple locations and geographies via email and other applications. The orginator or owner of the data often has little visibility or control over this.
- Notable sensitive data categories typically include; employee and customer personally identifiable information, confidential bnusiness financial and operational information, legal privilege information, operationalIT information, merger and acquisition information and business performance realted pre-release financial reports.

The Solution – Data Mapping Activity

Actions

- Identify – sensitive data assets.
- Classify assets – as to their value to your organisation.
- Discover – the loctions of the assets both electronically and physically.
- Report – collect, collate and evaluate this information so that assets can be tracked via a data asset inventory.

Summary of Requirements

As outlined earlier in the proposal, TfL require an extensive data mapping exercise to be performed, focusing on the organisation itself and a number of the external service providers. The exercise should focus on TfL’s personal data holdings and the associated data processing activities only.

The exercise will need to address the following questions about how personal data is being processed, together with the ICO GDPR Guidance (Accountability and Governance section) as follows: -

TfL Data Processing Questions

- *What personal data is being collected?*
- *How is that personal data being created / captured / collected?*
- *Why is that personal data being created / captured / collected?*
- *How is that personal data being used?*
- *Where is that personal data being stored?*
- *How is that personal data being secured?*
- *Who has access to that personal data?*
- *Who is that personal data being shared with?*
- *How long is that personal data being retained?*
- *How is that personal data being deleted / destroyed?*

Recital 82

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

Article 30: Records of processing activities

1. *Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*

    - *the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*
    - *the purposes of the processing;*

- *a description of the categories of data subjects and of the categories of personal data;*

- *the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*

- *where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;*

- *where possible, the envisaged time limits for erasure of the different categories of data;*

- *where possible, a general description of the technical and organisational security measures referred to in Article 32(1).*

2. *Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).*

3. *The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.*

4. *The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.*

Data Mapping - Approach

Identify

- What is the larger data category? (e.g., Personal, Financial, Business Operational, Legal).
- What is the sub category or data element? (e.g., Name, Address, DOB, Financial Records).
- What form is it in? (e.g. emails, forms, letters, spreadsheets, applications or database records).
- What is it used for and how is it processed?

Classify

- How valuable is the data? This is based on its Confidentiality, Integrity, and Availability (CIA).
- Impact? Would loss cause damage to individuals, business operations, or company reputation?
- Rate the data for an overall sensitivity rating.

Discover

- How data is typically generated or received?
- How is the data treated or processed?
- How is the data transmitted and to whom?
- Where is the data stored? Is it on a local device, in a database, in an application, hosted in the cloud, or with a partner?

Report

- Generate a comprehensive sensitive data inventory matrix from the information gathered.
- Report the executive summary findings along with any critical observations in a formal report.

Phase 1 – Project Planning and Preparation

The planning phase of this engagement is extremely important as it fundamentally affects the quality of the outputs.

The assignment begins with a Project Initiation Meeting attended by our Lead Consultant and TfL stakeholder(s). The purpose of the meeting is to:

- Reconfirm the scope of the project, the objectives, and deliverables.
- Agree relevant contacts and reporting lines.
- Agree timescales for delivery of the work.
- Confirm the staff and other contacts involved.

We will produce a Project Initiation Document for agreement by both parties and this will act as the key reference point for the project and will include an engagement plan/timetable.

Following on from the project initiation, the activities during the rest of this phase will include identification / confirmation of the following: -

- TfL Operating Subsidiaries (i.e. London Underground)
- TfL External Service Providers (who deliver outsourced operations on behalf of TfL), such as: -
    - Cubic Transportation Systems Ltd
    - Capita plc
    - NSL
    - Dawley Services Ltd
    - Marston Group
    - Independent Transport Associated Limited
    - Journeycall Ltd
    - Novacroft Ltd
- Key stakeholders / Interviewees, including: -
    - TfL Privacy and Data Protection Team
    - Personal Information Custodians - 60 Senior Managers with responsibility for systems and processes which are used to process personal data

- TfL Processes, including: -
  - Personal data – customer and internal (HR / employees)
  - GDPR Control Documentation
  - Current Information Risk Registers
  - Information Security Policy and Procedures
  - Information Security Organisation / processes
- Technology, including: -
  - Cloud service providers
  - Asset Registers
  - Network diagrams
  - Database schema
  - Operational Security Controls

Once we have validated all the relevant stakeholders, we will move forward with the following activities: -

- Hold an initial briefing session to communicate and explain the goals of the exercise and the cooperation required from your staff;
- Confirm the interviewees (Personal Information Custodians and 3rd parties), and issue a questionnaire to each interviewee to complete in advance. The aim of this is to initially identify data assets allowing a starting point for the data mapping;
- Agree the Data Mapping Questionnaire, which will as a minimum capture the following information:
  - Data Asset Types
  - Business Operations and Interfaces.
  - Data Record Volumes
  - Confidentiality, Integrity, Availability ratings to confirm sensitivity.
  - Resilience
- Issue Questionnaire to stakeholders two weeks in advance of interviews.

Prior to the on-site workshops we review and analyse the responses to the questionnaires provided by all the interviewees. This analysis provides a background to the interviews, and allows us to focus on identifying the data, the process, and the security controls.

Phase 2 – Data Mapping Assessment

The majority of this phase will consist of onsite workshops/interviews with key stakeholders and external service providers to cover the data flows of personal data across the organisation.

The workshops and interviews will identify the data asset, its use case, value and impact, processing transmission and storage conditions. As we progress through each interview, we consolidate our findings in the asset tracker and this will feed into the deliverables from the engagement (as detailed in phase 3 below).

During these onsite sessions, each process will also be identified and a data map generated. The data map will be iterative throughout the workshops to ensure accuracy.

The workshops can be run concurrently to shorten engagement time

Determining Data Sensitivity

Using a methodology defined in ISO 27005 we rate each data element on a scale of 1 (low) to 5 (high), based upon the following characteristics: -

- A) Data Value (or CIA rating) based the need for Confidentiality, Integrity and Availability in the event of:
    - Unauthorised Disclosure or Loss.
    - Unauthorised Modification.
    - Non-Availability of Data.
- B) Business impact with respect to:
    - Reputational Damage.
    - Financial Damage.
    - Loss of Operational Capability.
    - Consequences of Breach of Regulatory/Legal Requirements.
    - Cost and Effort Required to Mitigate Damage from Regulatory/Legal Breach.

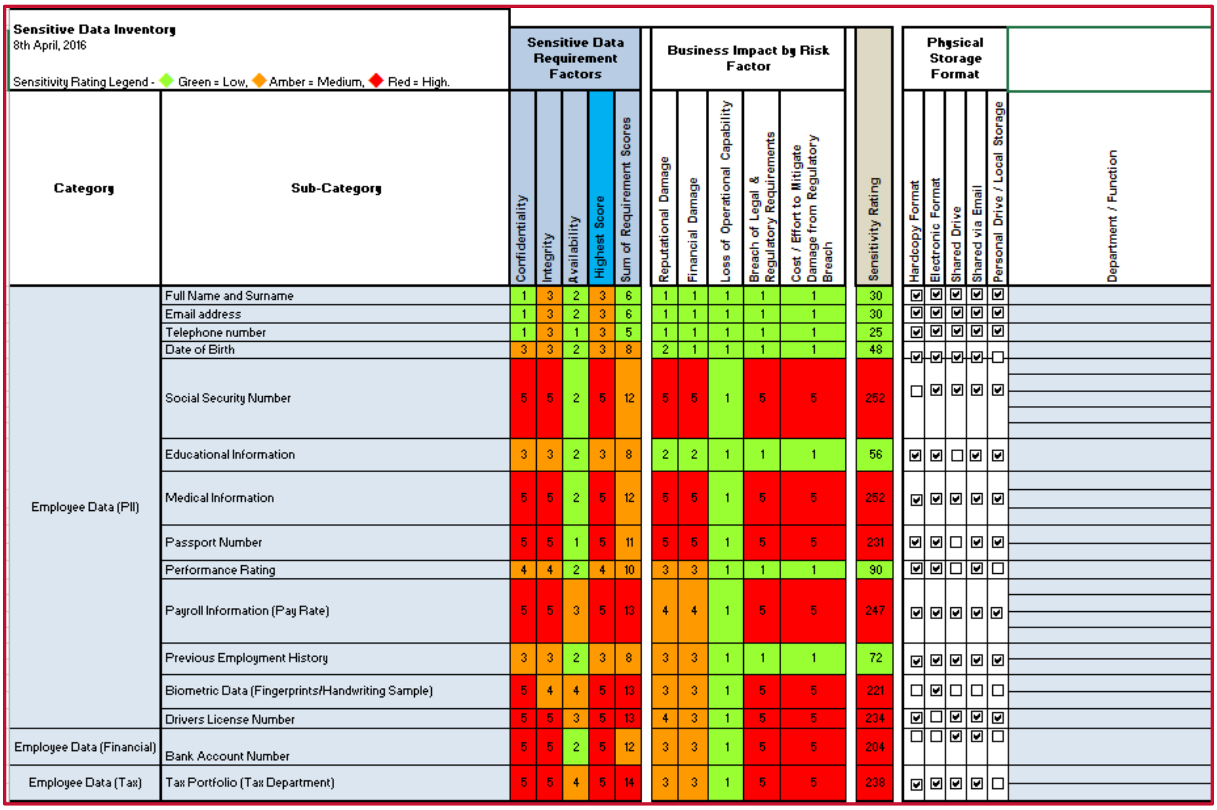
The overall sensitivity rating for each data element is determined by multiplying the scores from A and B above.

Phase 3 – Deliverables

Production of the formal deliverables will take place upon completion of workshop activities and will reflect the agreed output from the Project Initiation element of the project.

The typical deliverables we usually present as an output from the engagement include the following: -

- An Executive summary report based on the review delivered in PDF format, to include the approach used, the key findings and recommended way forward;
- Populated asset tracker/asset inventory in MS Excel defining the key assets by category, sub category, sensitivity rating and business impact rating, by department and by logical and physical storage location (example screenshot below)

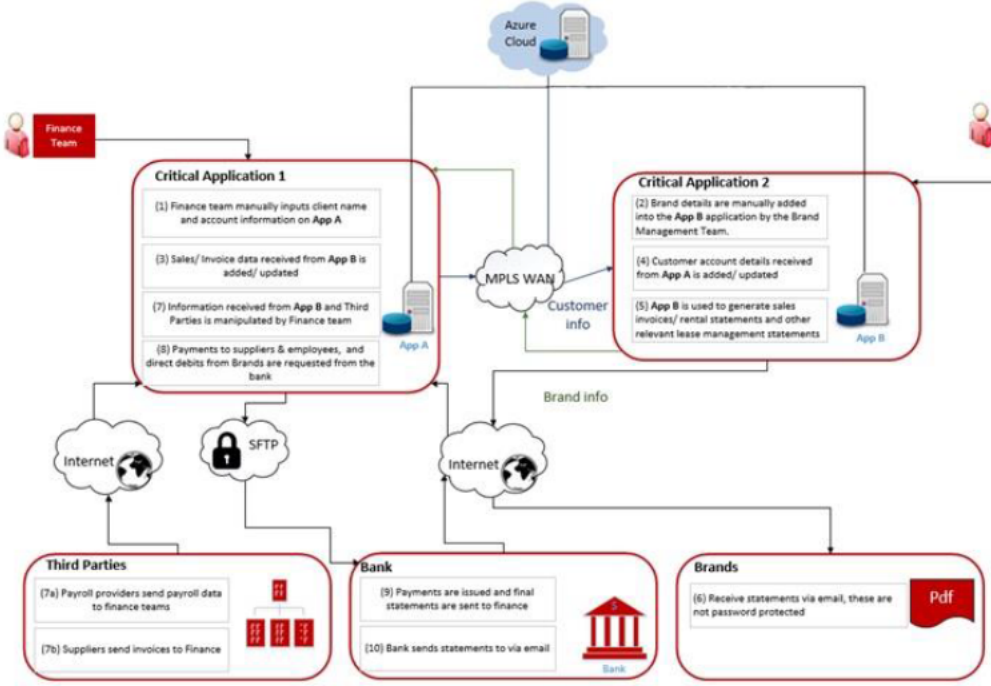


Sensitive Data Inventory
8th April, 2016

Sensitivity Rating Legend - 🟩 Green = Low, 🟧 Amber = Medium, 🟥 Red = High.

		Sensitive Data Requirement Factors					Business Impact by Risk Factor						Physical Storage Format					
Category	**Sub-Category**	Confidentiality	Integrity	Availability	Highest Score	Sum of Requirement Scores	Reputational Damage	Financial Damage	Loss of Operational Capability	Breach of Legal & Regulatory Requirements	Cost / Effort to Mitigate Damage from Regulatory Breach	Sensitivity Rating	Hardcopy Format	Electronic Format	Shared Drive	Shared via Email	Personal Drive / Local Storage	Department / Function
Employee Data (PII)	Full Name and Surname	1	3	2	3	6	1	1	1	1	1	30	☑	☑	☑	☑	☑	
	Email address	1	3	2	3	6	1	1	1	1	1	30	☑	☑	☑	☑	☑	
	Telephone number	1	3	1	3	5	1	1	1	1	1	25	☑	☑	☑	☑	☑	
	Date of Birth	3	3	2	3	8	2	1	1	1	1	48	☑	☑	☑	☑	□	
	Social Security Number	5	5	2	5	12	5	5	1	5	5	252	□	☑	☑	☑	☑	
	Educational Information	3	3	2	3	8	2	2	1	1	1	56	☑	☑	□	☑	☑	
	Medical Information	5	5	2	5	12	5	5	1	5	5	252	☑	☑	☑	☑	☑	
	Passport Number	5	5	1	5	11	5	5	1	5	5	231	☑	☑	□	☑	☑	
	Performance Rating	4	4	2	4	10	3	3	1	1	1	90	☑	☑	□	☑	□	
	Payroll Information (Pay Rate)	5	5	3	5	13	4	4	1	5	5	247	☑	☑	☑	☑	☑	
	Previous Employment History	3	3	2	3	8	3	3	1	1	1	72	☑	☑	☑	☑	☑	
	Biometric Data (Fingerprints/Handwriting Sample)	5	4	4	5	13	3	3	1	5	5	221	□	☑	□	□	□	
	Drivers License Number	5	5	3	5	13	4	3	1	5	5	234	☑	□	☑	☑	☑	
Employee Data (Financial)	Bank Account Number	5	5	2	5	12	3	3	1	5	5	204	□	□	☑	☑	□	
Employee Data (Tax)	Tax Portfolio (Tax Department)	5	5	4	5	14	3	3	1	5	5	238	☑	☑	☑	☑	□	

- Completed Questionnaires
- PII Data Inventory
- We have also included production of the Data Flow Diagrams (Visio) as an optional element within the investment – an example is shown below: -



(1) Finance team manually inputs client name and account information on **App A**

(3) Sales/ Invoice data received from **App B** is added/ updated

(7) Information received from **App B** and Third Parties is manipulated by Finance team

(8) Payments to suppliers & employees, and direct debits from Brands are requested from the bank

(2) Brand details are manually added into the **App B** application by the Brand Management Team.

(4) Customer account details received from **App A** is added/ updated

(5) **App B** is used to generate sales invoices/ rental statements and other relevant lease management statements

(7a) Payroll providers send payroll data to finance teams

(7b) Suppliers send invoices to Finance

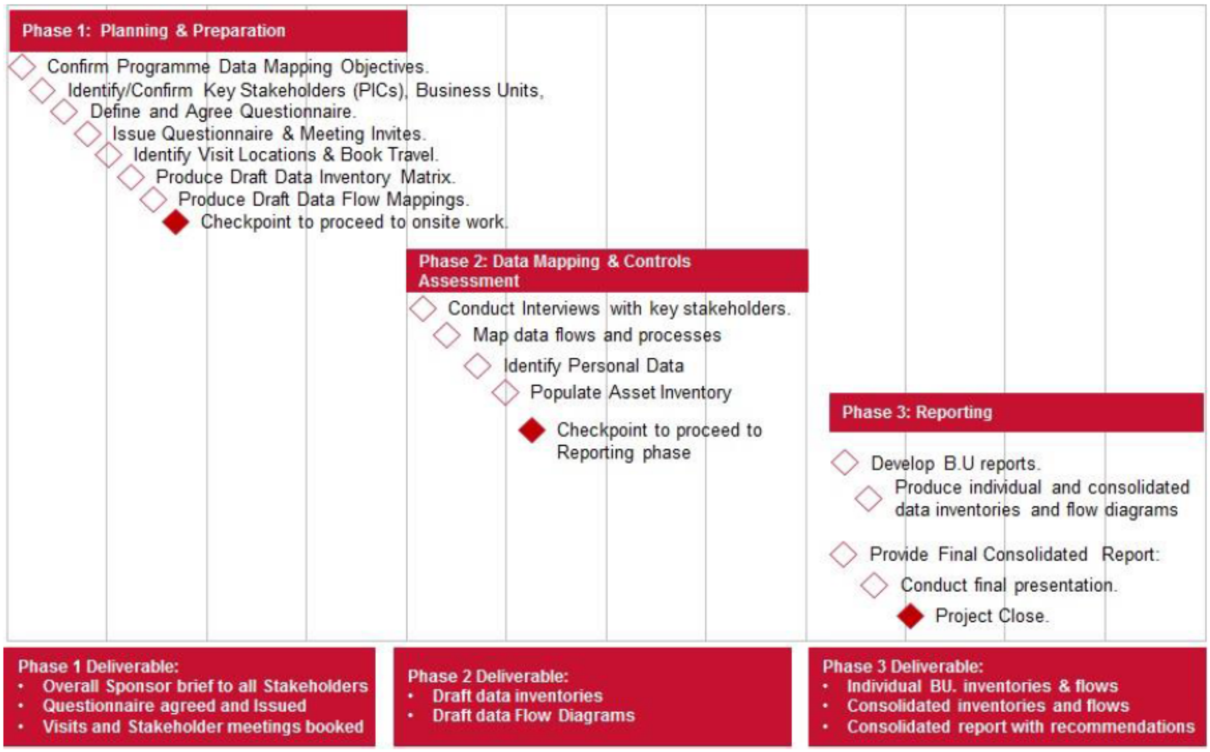
(9) Payments are issued and final statements are sent to finance

(10) Bank sends statements to via email

(6) Receive statements via email, these are not password protected

Programme Plan

The following programme plan is provided as an example but identifies the key stages and checkpoints of the engagement.



Phase 1: Planning & Preparation

◇ Confirm Programme Data Mapping Objectives.
◇ Identify/Confirm Key Stakeholders (PICs), Business Units,
◇ Define and Agree Questionnaire.
◇ Issue Questionnaire & Meeting Invites.
◇ Identify Visit Locations & Book Travel.
◇ Produce Draft Data Inventory Matrix.
◇ Produce Draft Data Flow Mappings.
◆ Checkpoint to proceed to onsite work.

Phase 2: Data Mapping & Controls Assessment

◇ Conduct Interviews with key stakeholders.
◇ Map data flows and processes
◇ Identify Personal Data
◇ Populate Asset Inventory
◆ Checkpoint to proceed to Reporting phase

Phase 3: Reporting

◇ Develop B.U reports.
◇ Produce individual and consolidated data inventories and flow diagrams
◇ Provide Final Consolidated Report:
◇ Conduct final presentation.
◆ Project Close.

Phase 1 Deliverable:

- Overall Sponsor brief to all Stakeholders
- Questionnaire agreed and Issued
- Visits and Stakeholder meetings booked

Phase 2 Deliverable:

- Draft data inventories
- Draft data Flow Diagrams

Phase 3 Deliverable:

- Individual BU. inventories & flows
- Consolidated inventories and flows
- Consolidated report with recommendations

Compliance Manager Tool

As outlined earlier in the proposal, TfL already use TRUSTe Assessment Manager to perform Data Protection Impact Assessments and other bespoke interactive compliance questionnaires.

Therefore, we would look to make us of this tool (where appropriate) during this engagement, and will agree the approach during Project Planning Phase 1.

Engagement process

Proposal Presentation

We understand that TfL are considering the data mapping exercise at this stage, and one of the aims of this proposal is to assist TfL in providing a business case / justification.

Therefore, NCC Group would also welcome the opportunity to present the proposal to the key stakeholders, so we can run through the programme in more detail and address any queries prior to a final decision being made.

During the Engagement

You will be allocated a lead consultant and a commercial account manager. They will be responsible for successful delivery of your project identifying and managing any issues. They will be accountable for ensuring that your project is assigned and completed to the expected standard and to the agreed timescales. All work is subject to our internal peer-review processes and quality assurance before being released.

We are committed to delivering a high quality service to you in line with our ISO 9001 quality management system, but in the unlikely event of an issue arising there are formal escalation procedures to help you quickly bring your issue to closure. Post-assignment reviews are carried out and the results are monitored by the PLC board.

Investment and return

This engagement will be delivered as a number of distinct phases. For simplicity, pricing for the project has been identified as separate items in the table below. All prices are subject to appropriate VAT but include expenses.

The investment is based on the information received to date and can be refined upon completion of the initial planning phase. Days will be delivered on a call-off basis so TfL will be invoiced only as the time is used – any remaining days can be rolled over for subsequent activity relating to the project.

Data mapping exercise and review of TfL	
Phase 1: Planning and Preparation – 10 days • Project Initiation • Programme Management (questionnaire development, reviews) • Scoping Workshops (up to 7 lasting 2-3 hours each)	[redacted]
Phase 2: Data Mapping Assessment – 60 days • Onsite visits to 10 x external service providers • Onsite interviews with key TfL Stakeholders (PICs) – up to 70 interviews and 250 questionnaires (each focussed on a different business unit/function encompassing multiple business processes) **(This can be refined upon completion of the planning activity)**	[redacted]
Phase 3: Deliverables and Reporting – 15 days • Development of Sensitive Data Inventory Matrix (Excel) • Executive Report (PDF)	[redacted]
Total investment	[redacted]

Data Flow Diagrams	
Production of Data Flow Diagrams – 1 day per diagram • Should TfL decide to go ahead with this element, we will confirm the number of diagrams to be produced during the planning activity. • Any days not utilised in the above table can be used for this activity	[redacted]

Pricing notes:

Cancellation charges

NCC Group retains the right to charge for income lost in the event of postponed or cancelled work, as set out in our Terms and Conditions.

Appendices supporting this proposal

Quality control

NCC Group is a global information assurance specialist providing organisations worldwide with expert escrow and verification, security consulting, web performance and domain services. We are committed to the profitable provision of services that anticipate and meet our customers' requirements and deliver excellent returns to our shareholders.

Achieving a high level of customer satisfaction is the target for all work. Profitability targets are set for each area of our business each month in an annual plan. Our overall effectiveness is measured by how well we perform against this plan.

This policy is supported by detailed measurable objectives in the form of Key Performance Indicators at all levels in the organisation structure. Performance targets are reviewed on a regular basis by management to ensure quality standards are constantly met and improved.

NCC Group operates a quality system of standards and procedures, which manages and controls all our projects, products, and service activities. The quality management system is based on the requirements of ISO 9001:2008, and is subject to continual improvement through our management review process.

The implementation of this policy is mandatory and is to be observed by all those who contribute to NCC Group's products and services.

Rob Cotton
Chief Executive Officer

January 2016

Terms and conditions

This proposal is subject to the terms and conditions of the Framework Agreement Number ITC11524 – Lot 1, signed between Transport for London and NCC Group Security Services Limited on 21st October, 2014.

Document

Issue number	Issue date	Issued by	Change description
0.1	15/02/2017	[redacted]	NCC Group internal proposal draft
0.2	15/02/2017	[redacted]	Revised QA
1.0	15/02/2017	[redacted]	Initial Proposal

Authorised distribution list

[redacted]	Senior Account Manager, NCC Group
James Alexander	Head of Privacy and Data Protection, TfL
Remi Williams	Commercial Manager, TfL

Document Version Control

Data Classification	Client Confidential
Client Name	Transport for London
Proposal Reference	P68030
Document Title	General Data Protection Regulation (GDPR) Compliance Programme - Personal Data Mapping Exercise
Author	[redacted]
Technical Approval	[redacted]
Commercial Approval	[redacted]

nccgroup
freedom from doubt