Data Protection Impact Assessment (DPIA)

Project Name:	Parking Services ICT & Re-Procurement
Project Manager or Sponsor (PM):	Shane Roberts
Name of person completing the DPIA if different to (PM):	
Service Team and Department:	Parking Services, Public Realm
Relevant Director and Executive Director:	Steve Iles
Information Management Champion(s) for service area:	Howard Passman
Date DPIA received by the IMT:	
Date approved by DPO:	
Date approved by IMT :	

1 Project Scope

You should describe here the nature, scope, context and purpose of the processed processing.

Reprocurement of the Parking back office ICT system and the potential sharing of data to enable bidders to effectively tender for the contract.

The DPIA for the project will also form the basis of the DPIA for the service when the successful supplier has been identified. The DPIA will be revised before contract award is confirmed to ensure that we have this in place before decommissioning, data migration and go live.

2 Data Description

Answer the questions below so that there is a clear understanding about how the information will be used, who will use it etc. Remember that it's personal information (i.e. information about individuals) that you need to be concerned with. If you do not have answers to all the questions at this time, simply record what you do know.

Whose information is being used? - *Are there additional concerns that need to be considered due to individuals sensitive/ complex circumstances? i.e. vulnerable person*	Registered Keeper details Customer Details Permit holder and applicant details
What information is being used? - *Consider the nature of this information E.g. Child's social care file*	• Registered Keeper details from the DVLA • Correspondence records • Permit holder and applicant details • Evidence provided by apellants to support Representations against Penalty Charge Notices (insurance details, medical information • Vehicle Registration Marks from ANPR / CCTV cameras & collected by Civil Enforcement Officers to issue (PCNs)
Does it include special category or criminal offence date?	No
Can an individual be identified easily from the information?	Yes
What is the potential impact on privacy of this information? - *What are the risks/ impact to an individual if this information was lost, stolen or manipulated?* - *E.g. could it be sold?*	Could be used to locate an individuals address and potentially allow access to details of other PCNs, which could give information as to the driver's likely routine, or where a driver has been.
Will this change the manner in which we handle, use or protect this information? *e.g. should it be encrypted?*	No Security in place to protect data held on the system,restricted access, passwords, PC encryption, GDPR training already in place.

3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	**14/05/19**
How did you consult individuals?	**Face to Face, HOS, team managers &**

	process experts
If not explain why it is not appropriate.	
Who else within the organisation have you consulted with?	**Information management via Legal instruction**
Do you need to speak with your processor to assist?	**No**
Do you plan to consult information security experts or any other experts?	**Council ICT to ensure system architecture supports compliance with GDPR before contract award**

4 Assessment of necessity and proportionality of data usage

What is your lawful basis for processing?	• Public Task • Legal Obligation
Is consent being relied upon to share the information? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?	No
Does the processing actually achieve your purpose?	Yes
How will the information be collected? Verbally, forms, intranet, interview, 3rd party, anonymous)	Correspondence, responces to statutory documents, Representations against PCNs, Internet, e-mails & telephone calls.
Is there another way to achieve the same outcome?	No
How will the information be used? *e.g. to write a report*	Issue and processing of PCNs Enforcement of unpaid PCNs Issue of permits
Do the individuals know and understand how their information will be used? If there are changes to their information does the privacy notice need to be amended?	Yes
How will it be stored, kept up to date and disposed of when no longer required? *e.g. stored in locked cabinet/securely shredded*	Data is kept on remotely hosted ICT back office system. Data is deleted after retention period.
How will you ensure data quality and data minimisation?	We are required to accept data in multi channels, however, investigating officers keep PCN processing information up to date as they become aware of any changes during investigations. Any linked cases are updated at the same time.
Who will have access to the information within LBC? - *Include approximate number of users*	PCN processing officers and management, Access Croydon, approximately 40 staff in total
Are there new or significant changes to the way we manage, use, handle or collect this information? - *Include any identified concerns for the individuals, would these changes heighten risks involved*	No
Will individuals within an existing database be subject to new or changed handling? - *If yes amendments need to be made to the privacy notice and these individuals need to be informed.*	No
What are the internal arrangements for processing this information? *e.g. number of staff who will have access*	Circa 40 staff
How will the information be updated? *e.g. monthly*	As cases are processed.

check	Identified DVLA make mismatches are redacted automatically
Does the project involve the exchange of information outside of the UK and are there set standards for how the information will be treated? How will you safeguard international transfers?	No
How will you prevent function creep?	Data is only used for the purpose enforcing and processing parking and traffic comntraventions and the issuance of permits. System is secure using passwords. Data cannot be lawfully shared with other council departments and used for other reasons.

5 Assessment of the risks to the rights and freedoms of data subjects

You must describe the source of risk and the nature of potential impact upon individuals and identify any additional measures to mitigate those risks.

5a Security

Who will be responsible for the control for this information?	Back Office ICT Provider (currently Conduent) Croydon, Parking Services
How will the access to this information be controlled?	Authorised access, secured by password protection
Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?	All officers with access to the data have had GDPR training and are aware of their responsibilities. Data is only disclosed to persons who have a legitimate reason to see it, such as the data subject, the Independent Parking Adjudication Service (ETA), Enfoercement Agencies collecting debt on our behalf or officers dealing with casework.
Are there adequate provisions in place to protect the information? If so what are they? *e.g. Process, security*	Security such as egress, SFTP , password protection. Parking use Neopost to provide tracking of printed documentsthrough the Royal Mail System and to ensure that the correct document is sent to the correct recipient.

5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	External Enforcement Agencies: • JBW • Phoenix • Newlyn • Equita • Whyte & Co • Ross & Roberts • Conferro Collections In order to collect outstanding debt as in the process specified in the Traffic management Act 2004 and other parking legislation • Internal Enforcement Agency Internal Debt Recovery Team & Croydon Gateway In order to collect outstanding debt as in the process specified in the Traffic management Act 2004 and other parking legislation Evidence is provided to ETA following an appeal by the Registered Keeper to the Independent Parking and Traffic Adjudicator. Evidence may be provided to the Local Government Ombudsman following a complaint by the Registered Keeper. The Registered keeper, who may request information from the council. Council External Legal – should we need to defend claims. Back Office ICT provider when data is entered / uploaded onto the ICT system.
What purpose does the information we are sharing have to the third party? - *Ensure that we only share relevant information and not excessively*	Details of who we believe to be the registered keeper of the vehicle and their location, in order that Enforcement Agencies can pursue unpaid debt. Where necessary, to rebut allegations of procedural impropriety and to defend the issue of the PCN.

Who will have access to the information, externally? - *Include approximate number of users* - *Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.*	Only those who have a legitimate need & under parking legislation. • ETA • LGO • External Enforcement Agencies Data (information) is transmitted using SFTP ICT Provider
How will it be transmitted to third parties and when? How often?	Only when required, this will depend upon the steps taken or not taken by the Registered Keeper.This will usually be by e-mail.
Is there a data sharing agreement in place?	External Enforcement Agencies and ICT Suplier are contractually obliged to handle data securely.
At what stage will the information be transferred?	Only at the appropriate point in the PCN Processing Cycle – Following an appeal following authorisation from Northampton County Court (TEC), or when there is a legitimate need to do so e.g. following .an complaint to the LGO.

5c Identified Risks and assessment:

You should take into account the sensitivity of the information and potential harm that inappropriate disclosure or use of the information could cause to any individuals concerned. You should also consider the reputational loss to the Council and the potential for financial penalties being imposed by the ICO.

To assess the level of risk you must consider both the **likelihood** and the **severity** of any impact on individuals. A high risk could result from either a high probability of some harm or a lower possibility of serious harm.

The severity impact level and likelihood should be scored on a scale of 1 to 10 with 1 being low severity and 10 high. The two scores should be **added** together. The RAG status is derived from the following scale:

Score:

- 15 to 20 = Red (High)
- 8 to 14 = Amber (Medium)
- Below 8 = Green (Low)

To be completed by Project Sponsor

Risk Identified	Severity of Impact	Likelihood of harm	Overall RAG rating
Data sent to back office system by CEO is inappropriately accessed by ICT provider	1	1	2
Data held on the back office system is inappropriately accessed by council staff	2	1	3
Information is disclosed by council staff to someone other than the Registered Keeper or Permit Holder	2	2	4
Information is processed incorrectly by back office staff, resulting in an incorrect address on statutory documents	1	3	4
Documentation is printed and enveloped incorrectly resulting in information being sent to someone other than the Registered Keeper	1	1	2

DVLA data sent to us to process in accordance with Parking and Traffic PCN processing is used for unauthorised purposes.	2	2	4
Permit Data is accessed by an unauthorised third party to find out an address for non-legitimate reasons	3	1	4
Sensitive data is released to a potential supplier as part of tender process	1	1	2

6 Identify measures put in place to reduce risk.

You must now identify additional measures you could take to reduce or eliminate any risk identified as medium or high risk in step 5.

To be completed by the Project Sponsor

Risk Identified	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated / reduced / accepted	Low / medium / high	Yes / No

Sign off and Record sheet

Item	Name/date	Notes
Measures approved by: Residual risks approved by:		Integrate actions back into project plan, with date and responsibility for completion. **If accepting any residual high risk must consult ICO before going ahead**.
DPO advice provided:		**Summary of DPO advice:** *(DPO should advise on compliance, measures to mitigate risk and whether processing should proceed)*
Consultation responses reviewed by:		If your decision departs from individuals views you must explain your reasons.
DPIA to be kept under review by:		Policy & Performance Manager

If you require further guidance to complete this DPIA please contact:

Information Management Team (IMT)
Ext: 47777
Email: information.management@croydon.gov.uk

Data Protection Officer
Email: DPO@croydon.gov.uk