Data Protection Impact Assessment (DPIA)

Project Name:	Uniform Re-procurement
Project Manager or Sponsor (PM):	Lelia Roche-Kelly
Name of person completing the DPIA if different to (PM):	Richard Wyatt-Jones (Business Analyst)
Service Team and Department:	Planning, Building Control & Strategic Transport Public Realm Housing Assessment & Solution
Relevant Director and Executive Director:	Heather Cheesbrough, Director of Planning, Building Control and Strategic Transport
Cost Code:	800138
Date DPIA received by the IMT:	11/5/2020
Date approved by DPO:	
Date approved by IMT :	

1 Project Scope

Croydon have been using the Uniform case management system, supplied by IDOX, for over 20 years. As a result, the Contracts Commissioning Board (CCB) require a formal open market review to ensure best value and transparency under the Public Contract Regulations is maintained. The core business areas currently using Uniform on a regular basis are:

- Development Management
- Building Control
- Licencing & Public Protection
- Housing Renewals

Uniform is used to manage and process applications received from members of the public for various licences types, ranging from specific business premises to personal licences and for planning permissions for property conversions or new developments. Applications are submitted voluntarily by applicants. Some application have prescribed content, some are discretionary and are worded to meet the various pieces of legislation applicable to the particular request. Most application forms will contain some element of personal information.

Teams can also receive written representations (objections) from residents and other interested parties. Under most legislation, an applicant is entitled to know the name and home address of any person who is objecting to their application. LBC will therefore seek consent from people raising objections to disclose their name and address to the applicant.

It is intended that this DPIA will act as generic and document covering the Uniform system as a whole, and will be revised and re-visited as the re-procurement process moves forward. Where available, examples have been included for illustrative purposes.

Once the tender is completed and a new provider(s) identified, service specific DPIAs will be required from each of the business areas listed above.

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*	Members of the public (Applicants) who wish to apply for various licences (both personal & commercial) and planning permission for property development work. Protection of vulnerable persons will follow current Council policies and procedures, as detailed in the Equality Assessment form already submitted.
What information is being used? - *Consider the nature of this information* *E.g. Child's social care file*	This will vary to meet the process / legal requirements of each team, but core data can include: Name, home address, date of birth, NI Number, confirmation of right to work, type of business, previous application histories
Does it include special category or criminal offence data?	Personal Licence applications require the submission of a basic Disclosure & Barring Service (DBS) form. Other applications require "Fit & Proper" person checks to be carried out.
Can an individual be identified easily from the information?	Yes. This information is also readily available from other sources e.g. Court records, the internet and local media.
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?*	The individuals voluntarily supply all the information required as they are applying for a licence, funding/assistance or planning permission. If information was lost, stolen or fraudulently manipulated, there could be

	the potential for applicants to be contacted, by companies or individuals wanting to target licencees, planning applicants or their businesses
Will this change the manner in which we handle, use or protect this information? *e.g. should it be encrypted?*	Not known at this stage. Data management and migration procedures are included as a mandatory requirement of the tender process.

3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	Under various pieces of current legislation, Responsible Authorities (RAs) are defined and listed. These can include the Police, LFB, City of London Veterinary Service, HMRC and potentially impacted members of the public, e.g. neighbours. Internal LBC teams such as Trading Standards & Children's Safeguarding can also act as RA's. Legislation requires applicants to send a copy of their application to each RA and, for certain applications, this information must be un-redacted so the documents will include personal information. If a local resident/other business want to see a copy of the application, the personal information of the applicant will be redacted first.
How did you consult individuals?	Applications are normally submitted via the Council portal(s) or in writing, with all supporting documentation either uploaded or provided as hard copies. All subsequent correspondence is managed via email or letter. Copies of all correspondence are retained for audit purposes and in accordance with prevailing data protection legislation and guidelines. Applicants may also have a duty to advertise their applications as public

	notices in the local media and at the proposed site.
If not explain why it is not appropriate.	N/A
Who else within the organisation have you consulted with?	Responsible Authorities can also be LBC internal teams, such as Trading Standards, Public Health, Children's Safeguarding and Development Management. The teams also consult with the Council's legal team when necessary.
Do you need to speak with your processor to assist?	Data Processors and other end users have been consulted when identifying and defining the new processes
Do you plan to consult information security experts or any other experts?	LBC Security & IM

4 Assessment of necessity and proportionality of data usage

What is your lawful basis for processing?	The council are legally obliged to process an applicant's data as part of the due diligence process to ensure that all necessary checks are completed, and any objections received are managed, prior to a licence or planning appilcation being granted
Is consent being relied upon to share the information? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?	Where there are statutory consultees, for example under the Licensing Act 2003, an applicant cannot decline to share their application with the relevant parties. If they do, the application will be declared invalid and rejected.
Does the processing actually achieve your purpose?	Yes.
How will the information be collected? Verbally, forms, intranet, interview, 3rd party, anonymous)	Submitted application forms (on line and hard copy) and letters/emails of objection.
Is there another way to achieve the same outcome?	Not at this time. All submissions and objections have to be made in writing
How will the information be used? *e.g. to write a report*	For the validation and recording the outcome of applications, and the maintenance of licencing and planning archives.
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?	Each piece of legislation sets out the statutory consultees and Responsible Authorities involved in the application process. Applicants are referred to the privacy notices posted on the Council website as part of the application process.
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 retention complies with all current data protection legislation and guidelines. Where some records (e.g. premises licences) need to be retained permanently, hard copies are stored securely off-site at LBC's archivists; Iron Mountain.

How will you ensure data quality and data minimisation?	Effective document management and scanning and Iron Mountain's storage/retrieval procedures.
Who will have access to the information within LBC? - *Include approximate number of users*	Relevant team members & senior officers across the 4 business units. (Circa 110 users). Inter departmental requests for information are processed on a case by case basis and are redacted where necessary.
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*	None anticipated at this stage (RP2)
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.*	It is intended that existing processes and procedures will remain in place. However this will be reviewed once the new vendor(s) have been appointed, and the service specific DPIA's created
What are the internal arrangements for processing this information? *e.g. number of staff who will have access*	Not known at this stage, but will vary between the individual business units. See Q4.10 above
How will the information be updated? *e.g. monthly check*	Licences are subject to renewal and ad-hoc change, e.g. due to transfer of ownership and / or variations to the licence conditions. This Information is updated as and when required
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?	All Data management processes and procedures will be reviewed, documented and communicated as part of the implementation of any new systems bought.

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?	Primarily, the individual Teams, along with the appointed vendor(s) and LBC Application Support Team
How will the access to this information be controlled?	Only people with LBC login details can access electronic records stored within the application.
Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?	Yes
Are there adequate provisions in place to protect the information? If so what are they? *e.g. Process, security*	LBC Digital Services systems and security procedures, in conjunction with the application's own security functionality.

5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	Copies of licences are shared with agencies such as the Police for enforcement purposes. As Relevant Authorities, they have seen all the personal information as it has been taken from the application forms, which they have received copies of. All RA correspondence is sent currently via email. However, the creation of a RA / Consultees dedicated portal for online communication is being considered as part of the new requirements.
What purpose does the information we are sharing have to the third party? - *Ensure that we only share relevant information and not excessively*	To enable the RAs to perform their enforcement & consultee duties.
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.*	The general public. RAs Other Local Authorities Health Authorities Central Government
How will it be transmitted to third parties and when? How often? - *Provide details of software used*	This will vary depending on individual Team's processes and the nature of information required and by whom. Again, this will be detailed in the service specific DPIAs

Is there a data sharing agreement in place?	Licencing comply with the 2003 Licencing Act's specific enforcement protocol that includes data sharing.
At what stage will the information be transferred?	On approval of a written request from a recognised / authorised party

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
Disclosure of applicant personal details to third parties not involved in the application process (name, home address, phone number, email address, details of previous convictions, details from passport extract)	5	3	8
Disclosure of personal details (name, home address and sometimes phone number or email address) without consent to applicant.	5	2	7
Disclosure of resident personal details (name, home address and sometimes phone number or email address) without consent to third parties not involved in the application process.	5	2	7

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** *Eliminated / reduced / accepted*	**Residual risk** *Low / medium / high*	**Measure approved** *Yes / No*
Disclosure of licence applicant personal details to third parties not involved in the application process (name, home address, phone number, email address, details of previous convictions, details from passport extract)	If a member of the public requests to see details of an application, they are entitled to know the name of the applicant but we would not disclose the home address, phone number or email address of an applicant to a Mop without the consent of the applicant. This information is redacted. Applications forms, licences and associated information are stored in digital form on the Council's digital networks and also in secure iron mountain storage. There are also hard copy files with the licensing team but only LB Croydon staff have access to this area.	Reduced & accepted	Medium	

Disclosure of resident personal details (name, home address and sometimes phone number or email address) without consent to applicant or third parties not involved in the application process.	We only disclose the name and address of an objector to an applicant if we have the written consent of the objector.	Reduced & accepted	Low	

Sign off and Record sheet

Item	Notes, **Name and date**
Measures approved by:	
Residual risks approved by: *(If accepting any residual high risk must consult ICO before going ahead.)*	
IM advice provided:	
DPO advice provided: *(DPO should advise on compliance, measures to mitigate risk and whether processing should proceed)*	
IM sign off:	
DPO final sign off:	

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