BARNSLEY
Metropolitan Borough Council

# Data Protection Impact Assessment Guidance and Template

# Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a **mandated** process designed to enable an organisation to analyse how a particular project or system will affect the privacy of the individuals involved. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice.

Any person who is responsible for introducing new or revised service or changes to a system, process or information asset is responsible for ensuring the completion of a DPIA.

A DPIA is suitable for a variety of situations which involve the processing of personal data, or to any other activity which could have an impact on people's privacy, the list below is not exhaustive but provides some examples.

Processing is any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

- A new IT system for processing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV)
- A new database which consolidates information held by separate parts of an organisation
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring
- A commissioned service who are processing data on the Council's behalf
- A renewal of any of the above, either by contract extension or via a waiver, where a DPIA was not previously completed

**When is a DPIA not required?**

A DPIA will not be required if the processing is 'not likely to result in a risk to privacy'. These are circumstances where no personal[1] or special category data[2] is being processed.

**To help you to identify whether a DPIA needs to be completed please answer the screening questions below. Once you reach a question where your answer indicates that a DPIA is not required, or for you to complete one or more of the stages, you do not need to answer the remaining screening questions.**

If you require advice and guidance please contact the Information Governance Team via the DigITal hub here.

## Screening Questions

[1] Personal data includes: name, address, identification number; location data; and an online identifier, DOB, phone number, Email Address, post code
[2] Special category data includes: race, ethnicity, religion, health data, political opinions, genetic data, biometric, trade union membership, sexual orientation

| **Project Name: First Homes** |
|---|
| **Project description:**<br>First Homes is a government policy to promote home ownership where private developers offer new homes at a discounted sale price. The scheme requires sharing - between the housing developer and the Council - of personal data about the potential purchasers. |
| **Information Asset Owner:**<br>Alison Dalton<br>Group Leader Strategic Housing and Growth |

**Screening Guidance:**

- Read each question carefully and compare your project against the examples provided to see if it sounds similar.
- Once you have answered YES to a question, you do not need to complete the remaining screening questions, the fourth column will tell you what to do next.
- Remember to sign and date the screening at the bottom of the list.

| Question | Context | Yes/No | DPIA? |
|---|---|---|---|
| 1. Are you procuring goods, equipment or software* where you will not be processing personal or special category data?<br><br>**OR**<br><br>Procuring or delivering a service that would not involve processing personal or special category data? | For example: procuring laptops, supply of goods e.g. food supplies, refurbishment of buildings, replacement goods e.g. fencing, maintenance e.g. water coolers, acquiring additional licenses for an existing system.<br><br>***If the software is web-based it is likely user data will be processed as a minimum, if this is the case please continue with the screening questions** | NO | If **YES -** no requirement for DPIA. Do not complete the remaining questions, sign below and submit to IG<br><br>If **NO -** continue to next question |
| 2. Are you procuring a commissioned service?<br><br>**OR**<br><br>Grant application | Also known as Outsourcing, this is where the Council commission another organisation to undertake the work on the Council's behalf. The organisation is the one who is collecting and processing the data on the Council's behalf (the Council may only receive auditing/aggregated data), however the Council needs assurance that appropriate technical and security measures are in place. To be a commissioned service the third party would act independently from the Council, and the council would not provide the third party with any personal data to assist them with the works. | NO | If **YES** complete stages 1, 3 and 4<br><br>If **NO** - continue to next question |

| | | | |
|---|---|---|---|
| | Example services: family time supervised contact, child protection advocacy, young people/carer support, maternity stop smoking scheme, sub misuse service, child protection advocacy. | | |
| 3. Are you collecting / processing[3] new personal, special category, criminal or data about people that could identify them?<br><br>Does the initiative involve processing personal data on a large scale? | This means if the information you are processing can distinguish an individual from other individuals, that individual will be identified. Personal includes name, address, identification number; location data; and an online identifier, DOB, phone number, Email Address, post code. Vulnerable may include children, employees, people with mental illness, asylum seekers, or the elderly etc. Special category data includes race, ethnicity, religion, health data, political opinions, genetic data, biometric, trade union membership, sexual orientation.<br><br>There is no specific definition of 'large scale' but the following should be considered: The number of individuals affected. The volume of personal data. The range of personal data. The duration or permanence of the processing activity. The geographical extent of the processing activity. Example implementing new customer / service user system. | YES<br><br>but not large scale | If **YES** complete stages 1, 2 and 4<br><br>If **NO** – continue to next question |
| 4. Does the initiative involve the procurement of a new system or software that is web-based? | This means that the system or software you are intending to use will be web-based (accessed via a web browser) and likely utilises cloud storage. Access to the system is likely to be granted via a username and password which would mean, as a minimum, user data is stored. | | If **YES** complete stages 1, 3 and 4<br><br>If **NO** continue to the next question |

[3] Processing includes: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

| | | | |
|---|---|---|---|
| 5. Does the initiative involve evaluating or scoring individuals (including profiling and predicting) or does the initiative involve systematic monitoring, or Does the initiative involve the use or application of innovative technological or organisational solutions? OR Does the initiative involve direct marketing? | Building behavioural or marketing profiles of individuals based on their web activity. Personal data processing used to observe, monitor or control individuals. Processing used to observe, monitor or control individuals - Installing a CCTV system, tracking location (online and offline), consider mobile apps which monitor. Using fingerprint recognition technology to control access to a building. Contacting individuals in a way they may find intrusive. For example emailing or telephoning without prior consent. | No | If **YES** complete stages 1, 2 and 4<br><br>If **NO** – continue to next question |
| 6. Are you using information about individuals for a purpose it is not currently used for, or in a way not currently used? **OR** Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | For example, data originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject<br><br>For example, processing of health data of residents in a joint project with another authority/organisation, new projects or a new service, or, delivering a service and commissioning an external partner to assist sharing data with them that they would not routinely have access to. | | If **YES** complete stages 1, 2 and 4<br><br>If **NO** – continue to next question |
| 7. Does the initiative involve automated decision-making that may have a significant effect on an individual? | Asking an individual to submit personal data that is then analysed by a computer system, with the result that the individual's request to use a service is either accepted or refused with no 'human' input, similarly to how most online credit card applications are processed. | | If **YES** complete stages 1, 2 and 4<br><br>If **NO** – continue to next question |
| 8. Does the initiative involve datasets that are to be matched or combined? | This relates to combining personal data originating from two or more personal data processing operations performed for different purposes or by different data controllers in a way that would exceed the reasonable expectations. Matching Council personal data against personal data held by a third party for profiling purposes. | | If **YES** complete stages 1, 2 and 4<br><br>If **NO** – continue to next question |
| 9. Does the initiative involve the transfer or storage of personal data in another country? | Sending or storing personal data to countries outside of the UK. For example, utilising a cloud storage service where the servers are hosted in the EU or USA. | | If **YES** complete stages 1, 2 and 4 |

| | | | |
|---|---|---|---|
| | | | If **NO** to all please contact IG |

| | |
|---|---|
| **Disclaimer -** If the answers indicate that there is no requirement to complete a DPIA you are taking responsibility for the decision. Forward to the IG Team via the DigITal hub who will store the document.<br><br>If the answers indicate a DPIA is required please proceed to complete the relevant stages below. Forward to the Information Governance Team via the DigITal hub who will assist in the review of the DPIA. | |
| **Name of completing officer:**<br>Sara Scholes | Date:<br>29/7/22 |

# DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

## Stage 1 – Full project details

**Stage 1a:** project detail (please provide as much detail as possible). If there are any documents e.g. business case that would assist IG to understand the project please attach

Who is the Project Owner?

Sarah Cartwright

Head of Strategic Housing, Sustainability and Climate Change

Who is the Information Asset Owner?

Alison Dalton

Group Leader Strategic Housing and Growth

Explain what the project aims to achieve

First Homes is a government policy to promote home ownership. Private developers offer new homes at a discounted sale price. The scheme requires sharing - between the housing developer and the Council - of personal data about the potential purchasers to confirm that all applicants meet the eligibility criteria. Eligibility criteria that must be proved includes; income, local connection and first time buyer status.

Explain what the benefits will be to the organisation

The Council is working with private developers to implement a new government policy.

Explain what the benefits will be to individuals and to any other parties affected

Successful applicants to the First Homes scheme will benefit from a discounted sale price. First Homes are sold with a minimum 30% discount, kept in perpetuity .

Does the project involve processing personal information?

Yes – to meet the criteria of the First Homes scheme, applicants are required to provide personal information including proof of income, first time buyer status and local connection.

## Stage 1b: objectives

Tick as many as applicable

☐Existing information to be used for a different purpose

☒New information sharing arrangement with an external company/organisation

☒New project involving collection and processing of people's information

☒New system/database

☐ Other: Click here to enter text.

## Now complete the key questions below

## Stage 2 - key questions

| | Question | Response |
|---|---|---|
| **Consultation requirements** | | |
| **1.** | **Internal consultation**<br>Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? | Already consulted with :<br>Governance and Compliance – DPIA and storage of data<br>Internal Audit – internal controls, storage of data<br>Legal – responsible for completing some key documents |

| | Question | Response |
|---|---|---|
| **2.** | **External consultation / engagement**<br>You should consider external stakeholder consultation. Outline timescales and method of seeking individuals' views or explain why it is not appropriate to do so. *External eg views of public)* | Has stakeholder engagement taken place: ☒ Yes ☐ No<br><br>If yes, which stakeholder and how have any issues identified by stakeholders been considered?<br>Homes England First Homes team – managing the early delivery First Homes pilot schemes in Barnsley. Provided templates for key documents and holding regular update meetings<br><br>Keepmoat and Gleesons – Private developers signed up for pilot scheme.<br>Other LAs – information shared with other councils on good practice<br><br>If no, explain why it was not appropriate to do so?<br>(Professionals, union representatives service users etc are useful to consult with or ask their opinion on the privacy implications of a project. You should put yourself in the individuals' shoes and envisage privacy implications.)<br>Click here to enter text. |
| **Data Items** | | |
| **3.** | **Please tick the information being used / collected**<br><br>**Personal**<br><br>**Special categories of data**<br><br>Quick Reference Guide to Personal & Special and/or Quick Reference Guide to Pseudonymisation | Who does the data relate to:<br>☐ Service User<br>☒ Member of Public<br>☐ Staff<br>☐ Other, please state:<br><br>☒ Name ☒ Address<br>☒ Phone number ☒ Email Address<br>☒ Post Code ☒ Date of Birth<br>☐ Pseudonymised Data ☐ Date of Death<br>☐ Unique Identifying Number ☒ NI Number<br>☐ Passport Number ☐ GP Practice<br>☐ Online Identifiers (e.g. IP Number, Mobile Device ID)<br><br>☐ Health Data ☐ Trade Union membership<br>☐ Political opinions ☐ Religion<br>☐ Racial or Ethnic Origin ☐ Genetic Data<br>☐ Biometric Data ☐ Sex life / sexual orientation<br><br>☒ Other: Income<br>Please consider data minimisation to ensure you are only collecting relevant information and not being excessive. |
| **4.** | **Please state reason for processing the information**<br>For example, providing a service, research, audit, evaluation. | To qualify to buy a First Home, applicants must prove they meet the criteria which includes: First Time Buyer status, household income <£80,000 , Mortgage covering at least 50% of discounted purchase price, local connection to Barnsley |

| | Question | Response |
|---|---|---|
| **5.** | **Is this information being used for a different purpose than it was originally collected for?** | ☐ Yes ☒ No<br>If yes, please state why and what legal basis you have for doing this:<br>Click here to enter text. |
| **6.** | **Approximately how many individuals' information will be collected?** | 15 applications included in the pilot scheme . Less than 100 applications expected per year for future years |
| **7.** | **Are you processing Children's data?**<br>**Quick Reference Guide to Processing Childrens Data** | ☐ Yes ☒ No |
| **Data processing** | | |
| **8.** | **Will another organisation outside the Council be processing the information?** | ☒ Yes ☐ No<br>If yes complete Q9 and Q10. If no, please go Q11 |
| **9.** | **Third party data processing** | Has a DPIA been completed by the organisation, if so please attach<br>Requested<br>Explain who in that organisation will have access to your data?<br>Housing Developer – sales, legal and conveyancing teams<br>What security arrangements do they have in place?<br>tbc<br>How does the processor demonstrate their compliance with GDPR?<br>tbc<br><br>If third party access is required to the BMBC network you are required to complete a Third Party Access agreement. If required, please copy the link to the entry in the register below:<br>Click here to enter text.<br>☒ Not Applicable |
| **10.** | **Is the organisation registered with the Information Commissioners Office?** | ☐ Yes ☐ No<br>Company name and Data Protection Reg Number: Information requested |
| **Information Security** | | |
| **11.** | **Describe who will have access to the information/system - internal and external?** | Limited number of BMBC Strategic Housing and Growth staff, BMBC Legal team |
| **12.** | **Is there a useable audit trail in place?**<br>For example, to identify who has accessed a record/system? | ☒ Yes ☐ No<br>☐ Not applicable<br>If yes, please outline the details: Click here to enter text. |

| | Question | Response |
|---|---|---|
| **13.** | **Detail where will the information will be kept/stored/transferred**<br>Please outline what data will be stored, where, and the use of any cloud storage | Information received from Housing Developers will be stored on BMBC sharepoint – access to the relevant folders will be restricted to a limited number of staff. An excel spreadsheet (password protected) will be used to monitor applications through the approval process. The monitoring spreadsheet is also filed in Sharepoint |
| **14.** | **Please indicate all methods in which will be transferred**<br>Quick Reference Guide to Transporting Information<br>Quick Reference Guide to Secure Email | ☐ Fax ☐ Email (Unsecure/Personal)<br>☒ Email (Secure) ☐ Internet (unsecure e.g. http)<br>☐ Telephone ☐ Internet (secure e.g. https)<br>☐ By hand ☐ Courier<br>☐ Post – normal ☐ Post – track/traceable<br>☐ Automatic System Transfer<br>☐ Other: Click here to enter text. |
| **15.** | **If you are transporting information, have you completed a Transporting Information Risk Assessment?**<br>E.g. if you are transporting data between the office and a service user's property. This data can be physical (printed copies) or digital (stored on a USB device or laptop hard drive). | ☐ Yes, please attach ☐ No<br>☒ Not applicable |
| **16.** | **Does the application/software have enhanced security?**<br>E.g. new forms of encryption; 2 factor authentication, pseudonymisation. | ☒ Yes ☐ No<br>If yes, please give details: Sharepoint – access restricted to a limited number of staff |
| **Confidentiality** | | |
| **17.** | **Please outline how individuals will be informed and kept informed about how their information will be processed**<br>e.g. Application Forms, Privacy Notices, Correspondence.<br>A copy of the privacy notice / link and/or leaflets must be provided.<br>Quick Reference Guide to Privacy Notices, Service Specific Privacy Notice and Quick Reference Guide to Individual Rights | Extract from First Homes Application form – see below – clearly states that data will be passed on to 3rd parties.<br><br>c. The homebuyer acknowledges that in order to process and administer your application [Developer] and the proposed First Homes Owner(s) mortgage advisor will pass over information you have provided over to 3rd parties the: [Local Authority], conveyancers, other government departments and agencies applicable for the purposes of processing this application and conducting statistical surveys and analysis of First Homes. |

| | Question | Response |
|---|---|---|
| **18.** | **Please select Lawful Basis for processing PERSONAL data.**<br><br>Please consult IG if considering selecting basis marked with *<br><br>**Quick Reference Guide to Legal Basis**<br>This interactive tool can help you to decide:<br>**https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/**<br><br>**Quick Reference Guide to Consent** | ☐ Contractual Obligation ☐ Public Interest<br>☐ Legal Obligation ☐ Vital Interest*<br>☐ Legitimate Interests*<br>☒ Consent (**if yes – provide details below**)<br>Is the consent explicit? ☒ Yes ☐ No<br><br>If yes how will consent be obtained and recorded?<br><br>Consent and permission to contact prospective buyers is included in the First Homes Application Form.<br><br>Consent will be obtained from the Housing Developer as part of the First Homes application process. |
| **19.** | **Please select Lawful Basis for processing SPECIAL category data.**<br>You may need to consult with BMBC Legal Dept<br>**Quick Reference Guide to Legal Basis**<br>**Quick Reference Guide to Consent** | ☐ Carrying out Obligations ☐ Data made public by data subject<br>☐ Protect Vital Interests ☐ Legal Claim<br>☐ Non-for-profit Body ☐ Archiving<br>☐ Substantial Public Interest ☐ Occupational Medicine (SOCIAL CARE)<br>☐ Public Health<br>☐ Explicit Consent (**if yes provide details below**)<br>If yes how will consent be obtained and recorded?<br><br>Consent and permission to contact prospective buyers is included in the First Homes Application Form.<br><br>Consent will be obtained from the Housing Developer as part of the First Homes application process.<br><br>**Not Applicable** |
| **20.** | **Will the processing of data involve means of automated decision making?** E.g. Asking an individual to submit personal data that is then analysed by a computer system, with the result that the individual's request to use a service is either accepted or refused | ☐ Yes ☒ No<br><br>If yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format). Click here to enter text.<br>Please also detail any profiling that may take place as part of the automated processing:<br>Click here to enter text. |

| | Question | Response |
|---|---|---|
| **21.** | **How will people's rights be managed e.g. if a request was made to erase data, restrict processing etc.**<br>**Quick Reference Guide to Individual Rights** | Requests can be made by First Homes applicants to either the Housing Developer or the Council. If a request is made before the verification procedure is complete, the Council will stop the process and advise the applicant that their First Homes application would be cancelled, and all personal information deleted. |
| **Data Sharing** | | |
| **22.** | **Does the project involve any new information sharing between the Council and another organisation?** | ☒ Yes ☐ No<br>If yes, please describe:<br>Information will be shared between the Council and any Housing Developers who are offering First Homes on their housing schemes. |
| **23.** | **Does the data sharing have any privacy enhancing technologies?**<br>New forms of encryption; 2 factor authentication, pseudonymisation. | ☐ Yes ☒ No<br>If yes, please give details: Click here to enter text. |
| **Privacy and Electronic Communications Regulations** | | |
| **24.** | **Will the project involve the sending of marketing messages electronically such as telephone, fax, email or text?** | ☐ Yes ☒ No<br>If yes, what communications will be sent?<br>Click here to enter text.<br>Will consent be sought prior to this?<br>☐ Yes ☐ No<br>If no, please explain why consent is not being sought first:<br>Click here to enter text. |
| **Records Management** | | |
| **25.** | **What are the specific retention periods for the information?**<br>Please refer to the Records Management Data Retention Schedule and list the retention period for datasets.<br>**Retention Schedules** | Suggested - Current + 12 years (based on RTB retention dates) |
| **26.** | **Will the information be securely destroyed or returned to the Council when it is no longer required?**<br>Dependent upon the contractual agreement | ☒ Yes ☐ No<br>If yes detail method of destruction OR return to Council: Click here to enter text.<br>If no, please detail: Click here to enter text. |
| **Information Assets and Data Flows** | | |

| | Question | Response |
|---|---|---|
| **27.** | **Who is the information asset owner (IAO)?**<br>Note it is the responsibility of the IAO to own the process/project and any risks identified.<br>The IAO should be an individual who is aware of, and/or ultimately responsible for the process/project. | Name of IAO: Alison Dalton<br><br>Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset?<br>☒ Yes ☐ No<br>If yes:<br>☒ Advise IAO to add to their Information Asset Register |
| **28.** | **A process flow map is required for all processing of personal information. Does a process flow map require completing or does an existing flow map need reviewing/amending?** | Does a new process flow map need completing?<br>☐ Yes ☒ No<br><br>Does an existing process flow map require reviewing/updating?<br>☒ Yes template ☐ No<br>Provided by Homes England for pilot scheme – will need to be reviewed at the end of the pilot. |
| **Publication of data** | | |
| **29.** | **Will identifiable information be released in to the public domain?** | ☐ Yes ☒ No<br>If yes, please describe: Click here to enter text. |
| **Data Processing Outside of the UK** | | |
| **30.** | **Will any personal and/or special data be transferred to a country outside the UK?** | ☐ Yes ☒ No<br>If yes, what data and to which country?<br>Click here to enter text. |

## Stage 3 - key questions for commissioned services, grant application or web-based systems/software.

**Note: Some answers will not be able to be completed until the service has been commissioned**

**Note: Only complete this section if you answered 'yes' to screening question 2 or 4**

**Note: Do not complete this section if you have completed Stage 2, only one of Stages 2 and 3 should be completed.**

| | Question | Response |
|---|---|---|
| **Consultation requirements** | | |
| **1** | **Has the external organisation/ system host completed a DPIA?** | ☐ Yes ☐ No<br>If no, why has one not been completed<br><br>If yes, please attach for review |

| | Question | Response |
|---|---|---|
| 2 | **Detail what information will be collected and where it will be kept/stored/transferred** | Click here to enter text. |
| 3 | **Please indicate all methods in which personal information will be transferred to the Council** | ☐ Fax ☐ Email (Unsecure/Personal)<br>☐ Email (Secure) ☐ Internet (unsecure e.g. http)<br>☐ Telephone ☐ Internet (secure e.g. https)<br>☐ By hand ☐ Courier<br>☐ Post – normal ☐ Post – track/traceable<br>☐ Automatic System Transfer<br>☐ Other:<br>☐ No personal information transferred to the council |
| 4 | **Please detail all relevant policies that are in place to support GDPR** | Click here to enter text. |
| 5 | **Is a signed contract or service level agreement in place to cover GDPR clauses? Note: this is a legal requirement** | ☐ Yes ☐ No<br>If yes, please attach for review.<br>If no, when will it be completed (an agreement must be in place)<br>Click here to enter text. |
| 6 | **Please detail any certifications the provider holds e.g. ISO27001, Cyber Essentials**<br><br>**Please detail the ICO registration number and name of organisation registered** | Click here to enter text.<br><br>Click here to enter text. |
| 7 | **Is any data processed or transferred outside of the UK?** | ☐ Yes ☐ No<br>If yes, what data and to which country?<br>Click here to enter text. |
| **Now please complete sections 4** | | |

## Stage 4: identify the privacy risks and solutions

A key part of the DPIA process is looking at risk and solutions, recording and identifying solutions to mitigate or reduce the risk. Appendix A can be used to identify the risks to individuals, corporate and compliance risks. Appendix B can be used to help identify the Data Protection related risks. You should think of solutions to reduce risks wherever possible. The result should be that the risk is either eliminated or reduced to an acceptable level of risk which the IAO is prepared to accept.

If you identify a high risk that cannot be mitigated, this DPIA must be sent to the ICO for consultation before starting the processing. Please liaise with the Information Governance Team who will be able to offer advice on this.

Please outline risks and solutions below. Risks identified should also be recorded and monitored on the appropriate risk register. Then using the 'severity of impact' table make an objective assessment of the risks. Consider the potential impact on individuals and any harm or damage the processing may cause – whether physical, emotional or material.

| Risk | Solution | Approved by | Indicator of risk H/L/M |
|---|---|---|---|
| Information is shared too widely or used for different purposes | Information initially shared by email – a new inbox has been set up with restricted access for named staff.<br>Information will not be shared with other council teams for any purpose other than validation of a First Homes application.<br>Security measures for documents and storage files to reduce risk of inappropriate use. | | Low |
| Lost or misplaced information | First Homes inbox to ensure all emails are in one location<br>Sharepoint files set up with restricted access for staff working on the scheme | | Low |
| Sharing of personal information not required for the First Homes application | Discussion with Developers providing personal information of what is required to meet the criteria of the scheme.<br>Excess information deleted and not filed. | | Low |
| Personal data kept on file in perpetuity | Retention period established | | Low |

| Severity of impact | | | | |
|---|---|---|---|---|
| | Serious harm | Low risk | High risk | High risk |
| | Some impact | Low risk | Medium risk | High risk |
| | Minimal impact | Low risk | Low risk | Low risk |
| | | Remote | Reasonable possibility | More likely than not |
| | | Likelihood of harm | | |

## Stage 5: review and approval

| | |
|---|---|
| **DPIA reviewed by Information Asset Owner (IAO) /Service Director / Head Of Service:**<br><br>***Note: it is the responsibility of the approving officer to own this process and to manage and monitor any risks identified within the DPIA*** | |
| Name: ALISON DALTON | Title: Group Leader Strategic Housing and Growth |
| Signed:<br>ADalton | Date: 01/08/22 |
| **DPIA reviewed by Data Protection Officer (DPO) if required (IG will advise):** | |
| Name: | Title: |
| Signed: | Date: |
| Summary of DPO advice: | |
| Review Date* ☒ 6 months ☐ 12 months Date Click here to enter text. | |

*You should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and reassess if anything changes. In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your DPIA assesses any new risks. An external change to the wider context of the processing should also prompt you to review your DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects.

## Appendix A

### Risks to individuals

- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.

- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

## Corporate risks

- Non-compliance with data protection or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

**Compliance risks** – Appendix B can also be used to help organisations identify data protection compliance

- Non-compliance with data protection.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

## Reducing Privacy Risk

There are many different steps which can be taken to reduce a privacy risk. This list is not exhaustive however some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

- Would the signing of a Non Disclosure Agreement (NDA) provide a solution to any potential data protection risks?

## Appendix B

## Linking the DPIA to the 6 Data Protection Principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with Data Protection or other relevant legislation, for example the Human Rights Act.

**Principle 1**

**Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals:**

You must have a valid lawful basis in order to process personal data. Please see Information Commissioner's Guidance for further details **Here**

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

**Principle 2**

**Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;**

Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

**Principle 3**

**Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

**Principle 4**

**Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay**

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

**Principle 5**

**Personal data processed for any purpose or purposes shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals**

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

**Principle 6**

**Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?