Data Protection Impact Assessment Procedures

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Dalmuir Park Housing Association

Data Protection Impact Assessment Procedure

Contents

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Overview

A Data Protection Impact Assessment ('DPIA') is a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the UK General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

We must do a DPIA for certain types of processing of personal data, or any other processing that is likely to result in a high risk to individuals.

A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

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

The Data Protection Lead will be consulted when completing a DPIA and where appropriate, individuals and relevant experts. Any data processors may also need to assist in completing it.

If we identify a high risk that we cannot mitigate, we must consult the Information Commissioner's Office ('ICO') before starting the processing.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

This procedure explains the principles and process that form the basis of a DPIA. It helps us to understand what a DPIA is for, when we need to carry one out, and how to go about it.

What is a DPIA?

A DPIA is a process designed to help us systematically analyse, identify and minimise the data protection risks of a project or planned change. It is a key part of our accountability obligations under the UK GDPR, and when done properly helps us assess and demonstrate how we comply with all of our data protection obligations.

It does not have to eradicate all risk, but should help us minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that we can apply to a wide range of projects regardless of size. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of strictness in proportion to the privacy risks arising.

Why are DPIAs Important?

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to £10 million or 2% annual turnover.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations. However, DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and Dalmuir Park Housing Association.

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information.

In turn, this can create potential benefits for our reputation and relationships with individuals:

- help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations;
- identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on; and
- reduce the ongoing costs of a project by minimising the amount of information we collect where possible and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within Dalmuir Park Housing Association and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a ‘data protection by design’ approach.

How are DPIAs Used?

A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA done by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of a DPIA back into any project plan. We should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help us manage and review the risks of the processing and the measures put in place on an ongoing basis. We need to keep it under review and reassess if anything changes. In particular, if we make any significant changes to how or why you process personal data, or to the amount of data we collect, we need to show that our DPIA assesses any new risks.

An external change to the wider context of the processing should also prompt us to review our 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 we do or the vulnerability of a particular group of data subjects.

What Kind of 'Risk' do DPIAs Assess?

There is no explicit definition of 'risk' in the UK GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we Need to do a DPIA?

We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan:

Systematic and extensive profiling with significant effects:

"any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person". **Large scale use of sensitive data:** "processing on a large scale of special categories of data referred to in Article 9(1) (See Appendix) or of personal data relating to criminal convictions and offences referred to in Article 10" **Public monitoring:** "a systematic monitoring of a publicly accessible area on a large scale".

The ICO has also published a list of the kind of processing operations that are likely to be high risk and also require a DPIA.

New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI). **Denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
Large-scale profiling: any profiling of individuals on a large scale.
Biometrics: any processing of biometric data.
Genetic data: any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
Data matching: combining, comparing or matching personal data obtained from multiple sources.
Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.

Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving any use of personal data.

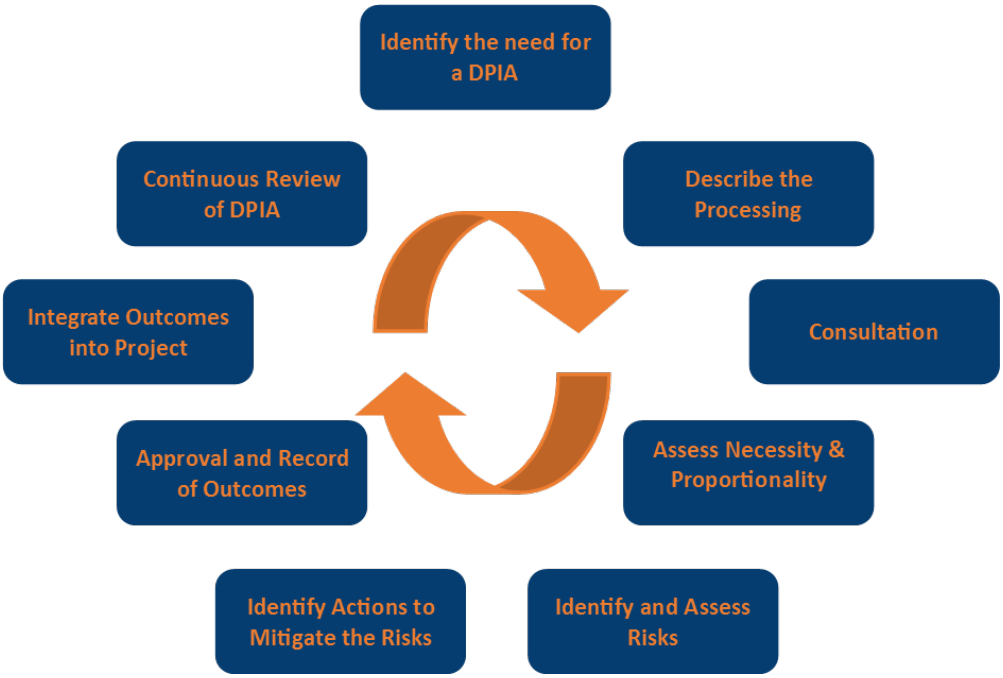
Responsibility for completing a DPIA

The project manager / lead would usually be best placed to conduct the required DPIA along with any other stakeholders who are able to input into the process.

The Data Protection Lead/DPO will have a significant role in supporting the process, providing advice and guidance, will approve any completed assessment and where required liaise with the Information Commissioners Office.

How to complete a DPIA

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



Step 1: Identify the need for a DPIA

1.1 Contact the Data Protection Lead /DPO and advise them of the new project/change.

1.2 Complete the DPIA Initial Screening Form to determine if you need to complete a full DPIA or a Mini-DPIA. .

1.2(a) If you decide that you do **not** need to do a full DPIA, you should document the decision and the reasons for it on the DPIA Initial Screening Form and complete the Mini-DPIA form.

1.2(b) If you **do** need to complete a full DPIA you should use the DPIA Template and follow the process from Step 2 below.

Step 2: Describe the Processing

2a Describe how and why you plan to use the personal data

The description must include "the nature, scope, context and purposes of the processing". The nature of the processing is what you plan to do with the personal data.

This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;

- who you share the data with;
- whether there are any data processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

2b The scope of the processing is what the processing covers.

This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

2c The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact.

This might include, for example:

- the source of the data;
- the nature of the relationship with the individuals (tenants, staff);
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern.

2d The purpose of the processing is the reason why you want to process the personal data.

This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole

Step 3: Consultation

You should always seek the views of individuals (or their representatives) unless there is a good reason not to.

In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of the DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

Do you need to consult anyone else?

If the project involves a data processor, you may need to ask them for information and assistance.

You should consult all relevant internal stakeholders, the IT Support Provider if this is a new system or change to an existing system to allow Information Security to be considered.

In some circumstances we might also need to consult the ICO once you have completed your DPIA. (Explained in Step 6)

Step 4: Assess Necessity and Proportionality

You should consider:

Do your plans help to achieve your purpose?

Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality.

In particular, you should include relevant details of:

- your lawful basis for the processing; (see Appendix - Conditions of Processing)

- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for any international transfers.

Step 5: Identify and Assess Risks

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material.

In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). You may wish to discuss these with the IT Provider for electronic data transfers.

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

The below Risk Matrix must be considered when assessing likelihood and severity of harm to the rights and freedoms of the individual.

Step 6: Identify Actions to Mitigate the Risks

Likelihood of Harm				
	PROBABLE	Low	High	High
	POSSIBLE	Low	Medium	High
	REMOTE	Low	Low	Low
		MINIMAL	SIGNIFICANT	SEVERE
	Severity of Harm			

What does 'harm' mean?

It is something that has an impact on an individual and can affect their circumstances, behaviour, or choices.

For example, a significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

Against each risk identified, record the source of that risk.

You should then consider options for reducing that risk.

For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

Record whether the measure would reduce or eliminate the risk.

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

When to consult the ICO

If you have identified a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. The focus is on the 'residual risk' after any mitigating measures have been taken. If the DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

How to consult the ICO

The DPO will consult with the ICO on Dalmuir Park Housing Association's behalf. This is done by completing the online form.

The submission must include:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- a copy of the DPIA;

You will be notified if the DPIA has been accepted for consultation within ten days of sending it. If the ICO agree that a DPIA was required, they will review the DPIA.

They will consider whether:

- the processing complies with data protection requirements;
- risks have been properly identified; and
- risks have been reduced to an acceptable level.
- The ICO will provide a written response, advising that:
- the risks are acceptable and you can go ahead with the processing;
- you need to take further measures to reduce the risks;
- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

In some cases, the ICO may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

If you disagree with the ICO advice you can ask for a review of the decision.

Step 7: Approval and Record of Outcomes

As part of the approval process, you should submit your assessment to the Named Role/DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

Step 8: Integrate Outcomes into Project

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

It is good practice to publish DPIA's to aid transparency and accountability. This could help foster trust in our processing activities, and improve individuals' ability to exercise their rights.

Step 9: Continuous Review of DPIA

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

EQUALITY, DIVERSITY & INCLUSION

We are committed to promoting an environment of respect, understanding, encouraging diversity and eliminating discrimination by providing equality of opportunity for all. This is reflected in our Equality and Human Rights Policy.

DATA PROTECTION

We will treat personal data in line with our obligations under the current data protection regulations and our Privacy Policy. Information regarding how data will be used and the basis for processing data is provided in our Board member Fair Processing Notice.

DISSATISFACTION

Although we are committed to providing high levels of service, we accept that there may be occasions where you may not be satisfied with the service you have received from us. We value all complaints and use this information to help us improve our services. Our Complaints Policy describes our complaints procedure and how to make a complaint.

Procedure Review

This procedure will be reviewed every three years or when required, by the Board of Management, to address any weakness in the procedure or changes in legislation or best practice.

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Appendix – Conditions for Processing

Below are the different legal bases available for processing personal data and special categories of data.

Legal Bases for Processing Personal Data:

6(1)(a) – Consent of the data subject (only use consent if there is no other condition that can be used)

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Categories of Special Category Data:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Conditions for Processing Special Categories of Data:

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-pro fit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.