Kunsill Lokali Ħal Tarxien

Data Protection Impact Assessment (DPIA) Policy

Policy Control

Drafted by:	[INSERT NAME]
Designation	[INSERT DESIDNATION]
Approved by:	[INSERT NAME]
Designation:	[INSERT DESIDNATION]
Date Approved:	[INSERT DATE]
Effective from Date:	[INSERT DATE]
Next Review Date:	[INSERT]

Version Control

Version No.	Date	Changes made by	Changes Details
1.0	[INSERT DATE]	[INSERT DESIDNATION]	DATA PROTECTION IMAPCT ASSESSMENT POLICY

Contents

1. Introduction

1.1. Privacy Legislation requires that, the Ħal Tarxien Local Council (hereafter referred to as the 'Council'), as a data controller, to consider and apply appropriate measures designed to implement their key principles effectively. Necessary safeguards must be integrated into all activities involving the processing of personal data to ensure the protection of the rights and freedoms of individuals. This is known as "Data Protection by Design".

1.2. An important element of the GDPR's focus on accountability and Data Protection by Design is the requirement to undertake a Data Protection Impact Assessment (DPIA) (also referred to as a Privacy Impact Assessment) where any processing of personal data is "likely to result in a high risk" to the rights and freedoms of data subjects.

1.3. Therefore, a DPIA serves as a tool to help Council to identify, evaluate and mitigate risks to individuals arising as a result of the processing of their personal data. At the same time, a DPIA should ensure compliance with data protection law and other legal and regulatory requirements.

2. About this Policy

2.1. This Policy sets out the Council's approach towards identifying the need for, carrying out, and implementing DPIAs.

2.2. Definitions of the terms used throughout this Policy can be found below.

Criminal Convictions and Offences	personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and Sentencing
Data Controller	the person or organisation that determines the purposes and means of processing personal data
Data Subject	an individual to whom personal data relates and who can be identified or is identifiable from personal data
GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679)
Personal Data	any information identifying or relating to a data subject that can be identified (directly or indirectly) from that data alone, or in combination with other identifiers possessed or that can be reasonably accessed. Personal data includes criminal convictions and offences data, special categories of personal

	data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently, irreversibly removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
Process, Processes, Processing	any activity or set of activities which involves personal data including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
Profiling	this means automated processing of data to analyse or to make predictions about individuals
Pseudonymised, Pseudonymisation	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms (e.g. a numerical code or key) so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that has been pseudonymised is still treated as personal data (unlike personal data which has been anonymised)
Special Categories of Personal Data	this means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy, personal data relating to criminal offences and convictions.
Vulnerable Persons	this means Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications.

3. Scope of this Policy

3.1. This Policy applies to all the Council's employees, contractors, companies and their departments.

4. Roles and responsibilities

4.1. All employees in the development of new data processing activities (referred to in this Policy as Activities) are responsible for ensuring that they are aware of this Policy and understand the circumstances in which a DPIA should be undertaken.

4.2. The [DESIGNATION] is responsible for overseeing and reviewing the implementation of this Policy and must be consulted in relation to any DPIAs undertaken in accordance with its requirements.

4.3. In practice, it is the responsibility of the employee leading an Activity to undertake the screening questions and produce the first draft of a DPIA if necessary, i.e. the project manager, system owner, etc. This must be carried out in collaboration with the Data Protection Officer, and other relevant stakeholders.

4.4. Draft DPIAs should be sent to the Data Protection Officer at dataprotection.tarxien@gov.mt for their endorsement or otherwise.

5. Identifying the need for a DPIA

5.1. A DPIA must be undertaken *before* the processing of any personal data which is "likely to result in a high risk to the rights and freedoms" of individuals such as but not limited to, installation of CCTV cameras in public places, processing involving biometric data, processing involving special category data, profiling, processing of data concerning vulnerable persons, processing of genetic data, use of innovative technologies etc. As such, it is necessary to identify whether there are any factors that warrant the need for a DPIA to be undertaken.

5.2. In the case of any Activities involving the processing of personal data that started before the 25th May 2018 (when the GDPR came into force) and which are still ongoing, such Activity should be reviewed and the need to undertake a DPIA considered.

5.3. The GDPR requires a DPIA to be undertaken where any Activity will involve:

a. the systematic and extensive evaluation of personal data by automated means, including profiling, resulting in decisions that would have significant effects for those individuals;

b. the processing of special categories of personal data or personal data relating to criminal convictions and offences on a large scale; or

c. the systematic monitoring of a publicly accessible area on a large scale.

5.4. Where any new Activity will involve the processing of personal data, the DPIA Screening Questionnaire should be completed. It is expected that the questionnaire will be completed by those leading the development of the Activity in collaboration with key stakeholders such as suppliers and potentially affected data subjects.

5.5. Before completing the questionnaire, it is important to:

a. identify the key stakeholders in the Activity so that they can provide their input into the questionnaire; and

b. have a clear understanding of the scope and objectives of the Activity so that the questionnaire can be completed as fully and accurately as possible.

5.6. If there is any uncertainty regarding completion of the questionnaire or the outcome, the Data Protection Officer should be consulted.

5.7. Where the outcome of the questionnaire suggests that the processing is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to:

a. the nature, scope, context and purposes of processing personal data;

b. the Councils of individuals affected by the processing (e.g. children or vulnerable adults);

c. the level of investment in the Activity in terms of time, financial and other resources; or

d. the visibility of the Activity internally and externally.

5.8. Where it has been concluded that a DPIA is unnecessary and will not be undertaken, the reasons for this should be clearly documented. The Screening Questionnaire should be retained to evidence the decision made and may need to be revisited and reviewed later.

6. Carrying out a DPIA

6.1. Having concluded that a DPIA is necessary or desirable for a particular Activity, the DPIA Template should be completed. The DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.

6.2. Part of the DPIA may involve consultation with relevant internal and external stakeholders. In the case of consultation with third party data processors, the contract with such third parties should include an obligation on them to provide assistance with carrying out DPIAs. However, this may have cost implications which should be considered and discussed with the third parties beforehand. In the case of consultation with professional advisers and other experts, the scope and cost of their involvement will need to be considered and approved by the [DESIGNATION].

7. Consultation with the Supervisory Authority

7.1. Where the outcome of a DPIA is that the processing of personal data in the context of an Activity would result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, the GDPR requires that the processing cannot commence before the Information and Data Protection Commissioner's office (**IDPC**) has been consulted.

7.2. The IDPC should not be consulted without the approval of the Data Protection Officer, who will usually initiate contact with the IDPC. Consultation with the IDPC should only be necessary in very exceptional instances as it is expected that the Council will be able to apply measures to appropriately mitigate or eliminate risk on most occasions.

7.3. The Data Protection Officer will contact the IDPC, sending a copy of the DPIA together with a cover letter to idpc.info@idpc.org.mt.

7.4. The IDPC will provide a written response confirming whether the risks identified are acceptable or whether further action is required. In some cases, the IDPC may recommend that the processing is not undertaken.

8. Review of DPIAs

8.1. A DPIA should be carried out at the earliest opportunity in the development of an Activity and re-assessed prior to commencement of the relevant processing activities to identify whether any changes to the Activity impact upon the outcomes of the DPIA and whether the controls and measures identified in the DPIA have been integrated into the Activity.

8.2. Once the processing of personal data has commenced in respect of an Activity, the DPIA should be reviewed regularly having regard to the nature and risks associated with the processing, taking into account any changes to the processing activities or scope of the Activity. A review should be undertaken at least annually by the employee leading or owning the Activity.

9. Disclosure and publication of DPIAs

9.1. There is no legal requirement to proactively disclose or publish a DPIA. However, it may be necessary to disclose a DPIA to another entity to provide assurance that due and proper consideration has been given to the data protection implications of an Activity.

9.2. A decision may also be taken to publish a DPIA in order to foster trust and confidence in the processing of personal data in relation to an Activity and to demonstrate accountability and transparency. However, such decision may only be taken in consultation with the [DESIGNATION], and any DPIA that is being published should be redacted to remove any confidential or commercially sensitive information.

10. Policy review

10.1. This Policy will be reviewed as required and at least every 2 years by the [DESIGNATION].