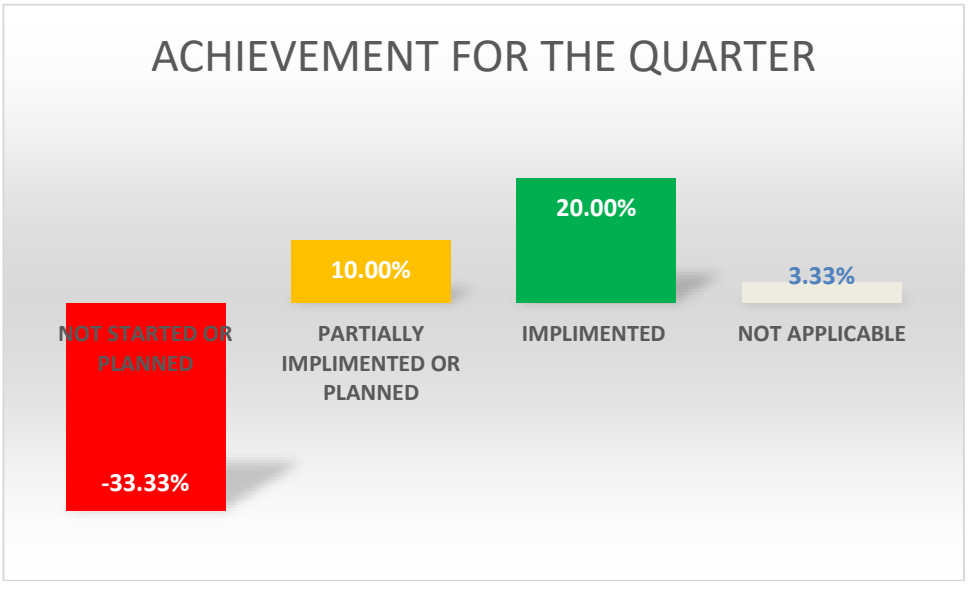
GDPR Review Report

Ħal Tarxien Local Council

Data Protection Officer: Adrian Mifsud

BOOM Consultancy & Advisory Services

T: 00356 79573417 E: adrian@boomconsultancy.eu



Overview of the GDPR and the Gap Analysis

Introduction to the GDPR

The General Data Protection Regulation (GDPR) and the majority of the provisions of the Data Protection Act (CAP 586 of the Laws of Malta) came into force on 25 May 2018: together this legislation (Data Protection legislation) replaced the Data Protection Act 1998.

The legislation introduces several major changes to former data protection legislation, including, but not limited to, increased accountability and transparency requirements, strengthened rights for individuals in relation to their own personal data, and greater penalties for breaching the requirements of the Data Protection legislation.

Moreover, all public authorities, including the Local Council, fall under the regime of the GDPR and are therefore held responsible to observe both European and local legislation related to data protection and privacy.

Objective of the Report

The objective of this report is to provide assurance of whether the Council has adequate arrangements in place, that are understood throughout the organisation, to protect the Council's information.

Scope of the Report

On the other hand, the purpose is to provide the Ħal Tarxien Local Council with feedback from the recent GDPR Gap Analysis Report and to identify areas of weakness and provide a framework, required to meet GDPR requirements over the next few months.

Administration of GDPR

There is a major requirement in GDPR to document everything done with personal data. This includes understanding where the data resides, what is held in the data, the sensitivity of data and the movement of data within and without the Local Council.

It must also be remembered that auditing the data, its use and sensitivity is not a one-off job but one which needs to be carried out on a regular basis.

The areas of GDPR that need to be administered are,

- Data Audit
    - What data is held where, types of data, sensitivity etc. Must also show the reasons for holding the data and when the data should be removed. This will be one of the company policies

- Data Transfers - A record of all data transfers for data processing. It must contain:
    - Data Source
    - Type of data
    - Name and address of Processor
    - Schedule of transfers (weekly, monthly etc.)

- Subject Access Requests – Keep a Record of
    - Right to Object

      Right to Restrict Processing
    - Right to Erasure
    - Right to Be Informed

- Data Breaches
    - What happened
    - When it happened
    - What Data was accessed
    - Whether data breach is serious enough to warrant informing data subjects.

- Record of DPIAs
    - a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
    - an assessment of the necessity and proportionality of the processing in relation to the purpose.
    - an assessment of the risks to individuals.
    - The measures in place to address risk, including security and to demonstrate that you comply.
    - A DPIA can address more than one project.

- Council Policies - These include:
    - name and details of organisation (and where applicable, of other controllers, representative and data protection officer);
    - purposes of the processing;
    - description of the categories of individuals and categories of personal data;
    - categories of recipients of personal data;
    - details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
    - retention schedules; and
    - description of technical and organisational security measures.

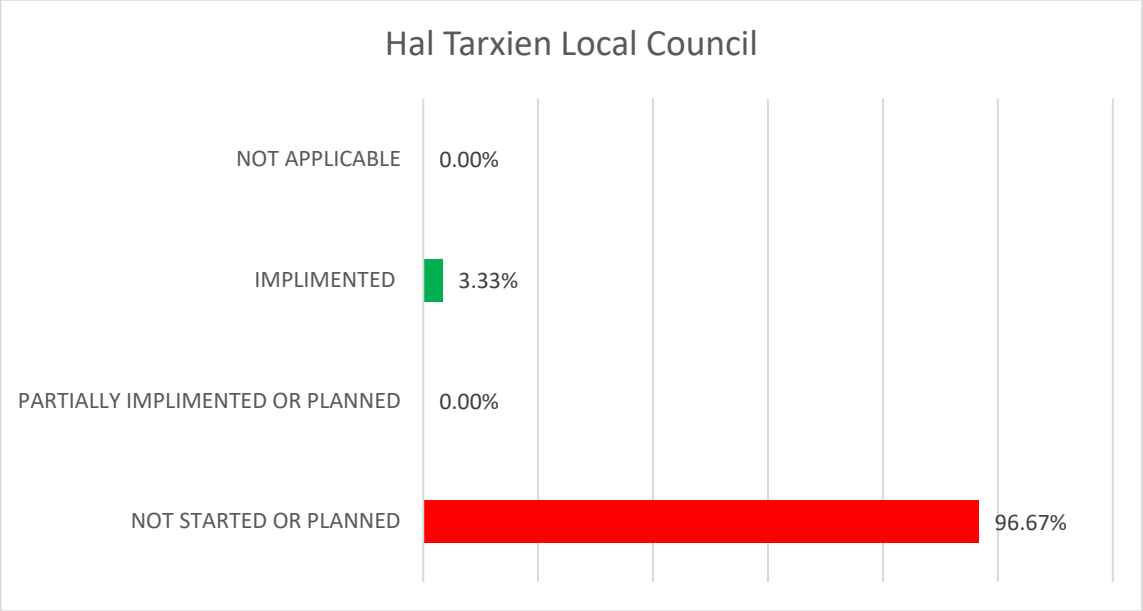
Progress registered till end of June

Appointment of Data Protection Office and the GDPR Gap Assessment
As from April 1st, 2019, Adrian Mifsud (BOOM Consultancy & Advisory Services) have been appointed as Data Protection Officer by the Ħal Tarxien Local Council. The IDPC was informed accordingly with the appointment.

The first task conducted was a GDPR Gap Analysis against thirty measures to commence the roadmap to GDPR compliance which a public authority must achieve as a standard requirement. Initials meetings with the Executive Secretary, being the Data Controller of the Local Council, and review of the operations related to all aspects falling under the scope of the GDPR.

As part of our brief as DPO, we performed the analysis with the assistance of the Executive Secretary on the 10th of April 2019.

An overview of the findings is shown below:



In general, the Gap Assessment found that the adequate policies and procedures were not in place. In order to enhance these, it was agreed to establish detailed procedures to commence with the drafting and approval of the main data protection.

Data Protection Principles

Data protection principles (which include the new GDPR data minimisation principles) require organisations to ensure that they only collect, process, and retain personal data required for their specific purposes; that they have sufficient personal data to properly fulfil those purposes; and that data held is periodically reviewed with anything not required deleted.

A good practice approach that ensures organisations have a complete record of all personal data held is to create and maintain a record of all data entered into the fields within all systems used, that could be linked with the GDPR record of processing. This approach can help to provide assurance in relation to compliance with data protection principles and individual rights.

Individual Rights

Due consideration was also given to highlight in our meetings that under GDPR an individual, or as known under the GDPR a data subject, has 8 defined rights:

- The right to be informed (privacy notices)
- The right of access (subject access)
- The right to rectification

- The right to erasure
- The right to restrict processing
- The right to data portability
- Rights in relation to automated decision making and profiling.

Henceforth one of the major tasks carried out in the time under review was to ensure that the Council is receptive to these rights and there comply with these fundamental rights that an individual enjoys by means of the GDPR.

The third major task for the period under review was to ensure that the Council complies to Article 28(3) of the GDPR require that where a data controller such as the Council uses a third party to process personal data (processor), the processing should be governed by a contract, binding the processor to the controller and setting out the subject matter and duration of processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

As DPO, we prepared a draft contract that the Council entered into with the respective data processors.

Data Protection Impact Assessments

The Council has a legal requirement to carry out a data protection impact assessment (DPIA) for any type of processing that is likely to result in a high risk to the rights and freedoms of individuals. A template for the completion of a DPIA is made available by the IDPC which however requires an additional risk assessment of the project in question. Further, the Council has to maintain an up-to-date register of all DPIA's in progress and completed, with these being sequentially numbered, to facilitate tracking of progress.

No DPIA was conducted or perceived to be conducted in the near future by the Council. Any DPIA shall obtain the confirmation that these had been fully completed, and that each was signed and approved as appropriate by the Data Protection Officer. This will then be referred to the office of the IDPC for further consideration.

Information Asset Register

Article 30 of GDPR requires that each controller shall maintain a record of processing activities under its responsibility.

That record shall contain all of the following: the name and contact details of the controller; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed (including internationally); details of transfers to a third country;

time limits for erasure (where possible); and a general description of the technical and organisational security measures (where possible).

The Council does not so far maintain an Information Asset Register. The processing activities are to be recorded in relation to personal data held was found to comply with the requirements of GDPR.

Data Retention

Article 5(1)(e) of GDPR requires that data should not be held for longer than it is actually needed. The Council must therefore have reasoning for the retention period for each item of data held.

The Council is to maintain a comprehensive data retention schedule which is easily accessible by all employees. Instruction for the method of disposal of the information is also to be given.

The Records Retention and Disposal Schedule is still to be compiled and the Data Protection Officer is assisting in the drafting of the policy, expected to be effective by the end of the second quarter.

The data breach process will be the next phase of compliance that the Local Council needs to address at the earliest. As DPO, we will endeavour to ensure that all systems are in place within the reporting period.

Review of the progress registered so far

Within the first three months of activity, the following policies, procedures and forms were implemented by the Local Council in compliance with the GDPR requirements:

- Data Processors Contracts
- Data Protection Policy
- Employment Privacy Policy
- Data Subject Request Form
- Data Subject Request Form Procedure
- Surveillance Cameras Policy
- Surveillance Cameras Data Subject Requests
- General Consent Form
- Filming/Photographic Consent Form

- Parental Consent Form
- General Withdrawal Consent Form
- Filming/Photographic Withdrawal Consent Form
- Parental Withdrawal Consent Form

Furthermore, the Local Council together with the Data Protection Officer implemented the following activities:

- Staff Awareness Poster Campaign

A Staff Awareness Training Session is still to be conducted.

Considering the implemented activities highlighted above, a comparison is being reproduced against the GDPR Gap Analysis measures as of April and the progress registered by end of June 2019.

The compliancy matrix is being based on:

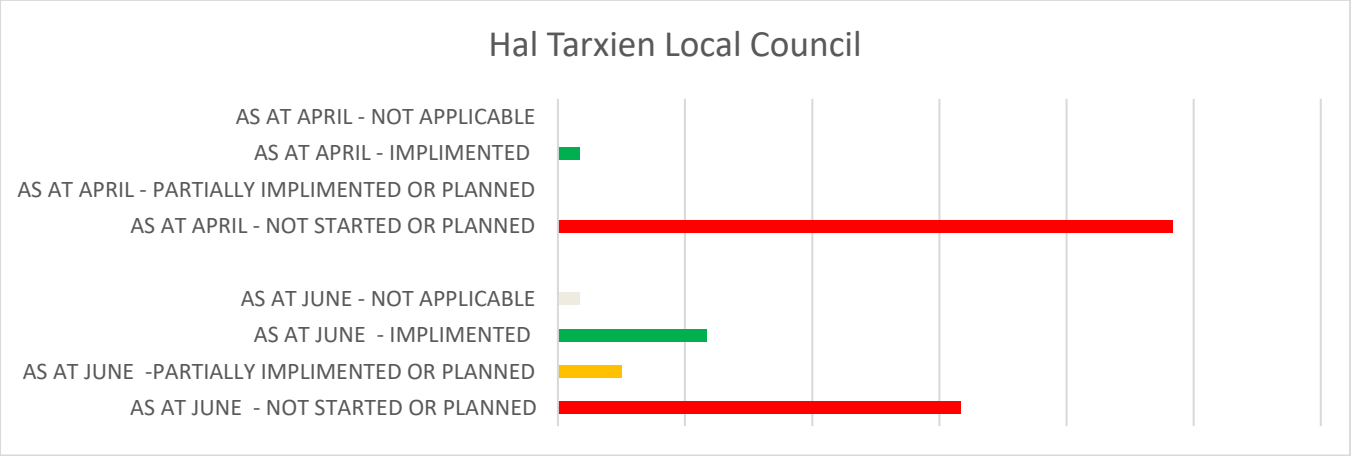
- **Green** means GDPR Compliant
- **Amber** means GDPR Partially Complaint
- **Red** means GDPR Not Complaint
- **Grey** means not applicable to the Local Council

	APRIL	JUNE
GDPR Measure	Hal Tarxien Local Council	Hal Tarxien Local Council
1. Conducted an information audit to map data flows.		
2. Identified your lawful bases for processing and documented them.		

3. Documentat of what personal data you hold, where it came from, who you share it with and what you do with it.		
4. Ask for and record consent.		
5. Systems to record and manage ongoing consent.		
6. Protection of vital interst of individual protected and documented.		
7. Legitimate interests as the lawful basis for processing considered and implimented.		
8. Communicates privacy information in a way that a child will understand.		
9. Has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way.		
10. Has procedure in place for processing operations constitute automated decision making under Article 22 of the GDPR.		
11. Monitors its own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.		
12. Provides data protection awareness training for all staff.		
13. Manages information risks in a structured way so that management understands the Local Council impact of personal data.		
14. Your Local Council has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.		
15. Understands when you must conduct a DPIA and has processes in place to action this.		
16. A DPIA framework is in place to link the existing risk management and project management processes.		
17. Has an information security policy supported by appropriate security measures.		
18. Has an adequate level of protection for any personal data processed by others on its behalf that is transferred outside the European Economic Area.		
19. Has effective processes to identify, report, manage and resolve any personal data breaches.		
20. Privacy information readily available to individuals.		
21. Established a process to recognise and respond to individuals' requests to access their personal data.		
22. Has processes in place to ensure that the personal data you hold remains accurate and up to date.		

23. Has a process to securely dispose of personal data that is no longer required or where an individual has asked for it to be erased.		
24. Has procedures to respond to an individual's request to restrict the processing of their personal data.		
25. Has procedures to handle an individual's objection to the processing of their personal data.		
26. Has a written contract with any processors you use.		
27. Decision makers and key people in your Local Council demonstrate support and promote a positive culture of data protection compliance.		
28. Has an appropriate data protection policy.		
29. Has systems to mange the consent to offer online services directly to children.		
30. Has appointed a DPO.		
Total Red	29	19
Total Amber	0	3
Total Green	1	7
Total Grey	0	1

Considering the above achievements, the Local Council has made inroads in GDPR compliance. A comparison between the rate of compliance in April and in June, is demonstrated below:



From the above, it could be noted that considering the first three months of activity, the Local Council has managed to increase its level of GDPR compliance with a favourable prospect

that in the coming months it will be able to attain a high level of compliancy.

Although the rate of compliance is still relatively low, standing at 23%, partially compliant is 10%, leaving 63% as still not complaint to the GDPR.

A significant progress of GDPR compliance can be registered, being 20%.

Concluding, the GDPR is designed to further protect the personal data of individuals. This will require significant investment of time and money. However, these changes will also enable businesses to think more carefully as to how they interact with their customers and in the long term may well improve customer relationships with increased trust and a respect for personal privacy.

Getting it wrong is not an option.

Limitations of Scope

Work performed in the compilation of this report did not include the following areas in scope:

- Our review was limited to the design of the GDPR Gap Assessment and did not cover control effectiveness. Consequently, no detailed testing or deep dives into specific areas was performed to confirm the accuracy of gap analysis assessments;

- Only those processes and policies within the control of the Council were included in scope. No work was performed to assess the extent of third-party supplier compliance with GDPR requirements; and

- The finding and comments within this report does not guarantee that the organisation will be fully compliant with GDPR requirements.