#1 of 9 – What is a DPIA?

- A process that aims to identify and minimise the privacy risks of any given data processing activity.

- In summary, a DPIA must include details such as –
  - a description of the data processing including its purposes;
  - an assessment of the necessity and proportionality of the processing;
  - an assessment of the risks to individuals; and
  - the measures envisioned to mitigate the risks.

- Please see pp.1-2 of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#2 of 9 – When is a DPIA required?

- A DPIA should be performed only when the processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

- A processing meeting two of the below criteria would generally be high risk and require a DPIA :
  - evaluation or scoring;
  - systematic monitoring;
  - sensitive data;
  - data concerning vulnerable data subjects; or
  - innovative use of technological or organisational solutions.

- Please see pp.4-6 of Guidance Note IR04/17 (4) “Data Protection Impact Assessment” for further information on the above: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#3 of 9 – When is a DPIA not required?

Circumstances in which a DPIA is not required:

- Where the processing is not likely to result in a high risk to individuals.
- When the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has already been carried out.
- The results of the existing DPIA may be used.
- Where a processing operation has a legal basis in EU or Gibraltar law and has stated that an initial DPIA does not have to be carried out.

Please see p.8 of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#4 of 9 –Examples

Examples demonstrating how specific types of data processing may or may not meet relevant criteria for a DPIA:

DPIA Required		DPIA Optional (not required)	
Camera on roads using intelligent video analysis to automatically recognise number plates	Systematic monitoring Innovative technology	Lawyer processing client personal data	Sensitive/highly personal data Vulnerable data subjects
Company monitoring employees activities (CCTV, internet activity etc.)	Systematic monitoring Vulnerable data subjects	Website displaying adverts involving limited profiling based on past purchases	Evaluation or Scoring
Hospital processing patients' genetic/health data	Sensitive/highly personal data Vulnerable data subjects Large scale	Online magazine using mailing list to send generic digest to subscribers	Large scale

Please see p.7 of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

For more information or advice please contact our office.

privacy@gra.gi (+350) 200 74636

GRA GIBRALTAR REGULATORY AUTHORITY

DPIA Data Protection Impact Assessment

#5 of 9 – Existing processing operations

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

- A DPIA is required for processing operations introduced after the GDPR becomes applicable on 25 May 2018.
- In regards to existing data processing activities, a DPIA is required when significant changes occur.
- The Commissioner recommends that DPIAs are conducted for processing operations started prior to May 2018.
- Please see pp.8-9 of Guidance Note IR04/17 (4) “Data Protection Impact Assessment” for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#6 of 9 – Who should carry out a DPIA?

- The data controller is responsible for ensuring that a DPIA is carried out.
- The data controller can consult and seek assistance from the Data Protection Officer ("DPO") and the data processor.
- The data controller must also seek the views of data subjects or their representatives where appropriate.
- The following can also be consulted - relevant business departments; professionals e.g. lawyers, technicians, security experts, sociologists, etc.; and the Chief Information Security Officer (if appointed) and/or the IT department.
- Please see p.11 of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#7 of 9 – Carrying out a DPIA

- It is up to the data controller to choose a DPIA methodology.
- The below is an example of a DPIA methodology –

Step 1: identify the need for a DPIA in relation to the envisaged processing operations and purposes (where applicable, the legitimate interest pursued by the controller);

Step 2: assess necessity and proportionality of the processing;

Step 3: identify the privacy and related risks to the rights of individuals;

Step 4: identify and evaluate the measures to address risks (privacy solutions);

Step 5: sign off and record/document the DPIA outcomes to demonstrate compliance; and

Step 6: integrate the outcomes into the project plan.

Please see p.12 and ANNEX A of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#8 of 9 – Publishing the DPIA

- Publishing a DPIA is not mandatory under the GDPR.

- However, publishing it can help foster trust in the data controller's processing operations and demonstrate accountability and transparency.

- Publication of the DPIA does not need to contain the whole assessment:
  - it can contain a specific part of a DPIA;
  - it can be in the form of a summary of the DPIA's main findings;
  - or a statement can be published announcing that a DPIA has been carried out.

- Please see p.12 of Guidance Note IR04/17 (4) "Data Protection Impact Assessment" for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636

#9 of 9 – Consulting the Supervisory Authority

- The Commissioner must be consulted if residual risks are high and data controllers are unable to mitigate risks when conducting a DPIA.
- Regardless of whether consultation is required, an organisation will still need to meet their obligations of retaining a record of the DPIA and keeping it up to date.
- Please see p.13 of Guidance Note IR04/17 (4) “Data Protection Impact Assessment” for further information: www.gra.gi/guidance-on-the-general-data-protection-regulation/gdpr4

GRA
GIBRALTAR REGULATORY AUTHORITY

DPIA
Data Protection Impact Assessment

For more information or advice please contact our office.
privacy@gra.gi (+350) 200 74636