

In terms of Article 35(4) of the General Data Protection Regulation, supervisory authorities shall establish and make public a list of the kind of processing operations which, taking into account the nature, scope, context and purposes of the processing and, in particular, when using innovative technologies, are likely to result in a high risk to the rights and freedoms of natural persons. For such activities, prior to the processing, controllers shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The Maltese Data Protection Authority has established the following processing operations where a Data Protection Impact Assessment (“DPIA”) shall be required to be carried out by controllers prior to the processing.

For the purposes of ensuring consistency across the Union, the list of the kind of processing operations has been established after taking into account the guidelines on DPIAs¹ that were adopted by the WP29 and subsequently endorsed by the EDPB. The list is non-exhaustive in nature and shall complement and further specify such guidelines.

1. **Systematic monitoring – Criterion 3 of WP248** : processing of personal data that involves:
 - a. observing, monitoring or controlling data subjects’ behaviour, in particular, on the online environment;
 - b. specific circumstances where the controller is legally required to process personal data about data subjects without their knowledge;
 - c. operations concerning the use of geolocation data, including but not limited to, for the purpose of direct marketing; or
 - d. monitoring on a large scale of public spaces or private areas accessible by the public.
2. **Automated-decisions - Criterion 2 of WP248**: fully or partially automated means of processing, including profiling, which produces legal effects concerning the data subjects or similarly significantly affects them.
3. **Use of innovative technologies - Criteria 4 & 7 of WP248**: any processing of special categories of personal data and of data concerning vulnerable data subjects, through the use of innovative technologies or the implementation of new methods in existing technology.
4. **Special categories of data - Criterion 4 of WP248**: processing on a large scale of special categories of data, including, personal data relating to criminal convictions and offences.
5. **Biometric data - Criteria 4, 3 & 7 of WP248**: any processing activity involving biometric data for the purpose of uniquely identifying data subjects:
 - a. when the data subjects are in a public space or in a private area accessible to the public;
 - b. when the biometric data are processed in conjunction with personal data related to criminal convictions and offences;
 - c. when the biometrics are related to individuals who need high protection such as minors, employees, patients, mentally ill persons and asylum seekers.

¹ WP 248 rev.01 - Guidelines on the Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, as last revised and adopted on 4th October 2017.

6. **Genetic data - Criteria 4 & 6 of WP248:** any processing of genetic data, other than that processed by an individual health care professional when providing a related service directly to the data subjects, for the purpose of matching or combining datasets in a way that would exceed the reasonable expectation of the data subject.

7. **Data concerning vulnerable persons - Criterion 7 of WP248:** processing of personal data of vulnerable natural persons, in particular, concerning children, employees and individuals receiving any form of social assistance.

8. **Employee monitoring – Criteria 1 & 7 of WP248:** processing of personal data for the purpose of the evaluation or scoring of aspects concerning the employee’s performance at work, or when the processing increases the power imbalance between the data subjects and the data controller, particularly, when the employees may be unable to easily consent to, or oppose, the processing of their data or exercise their rights.