Where data processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall carry out a data protection impact assessment before starting the data processing. Under Article 35 (4) of regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter 'the GDPR'), the National Authority for Data Protection and Freedom of Information (hereinafter 'the NAIH') established a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment, and makes it public hereunder.

The NAIH calls the attention of data controllers to the fact that it is their general obligation to assess and appropriately manage to mitigate the data protection risks of their data processing operations even beyond those included in the list. Carrying out a DPIA does not exempt the controller from the obligation to comply with other obligations of the GDPR or other obligations contained in sector-specific or general legislation. The list below is by no means exhaustive: carrying out a DPIA shall always be required as soon as the conditions stipulated in Article 35 (1) of the GDPR have been met. Beyond the mandatory cases provided in Article 35 (1) and (3) of the GDPR—taking also into account the exceptions under Article 35 (10) of the GDPR—data controllers shall carry out a data protection impact assessment in the following cases of data processing:

1) Where the processing of **biometric data for the purpose of uniquely identifying a natural person** refers to systematic monitoring.
2) Where the processing of **biometric data for the purpose of uniquely identifying a natural person** concerns vulnerable data subject, in particular, concerning children, employees, and mentally ill people.
3) Where the processing of **genetic data** is carried out in connection with sensitive data or data of a highly personal nature.
4) The purpose of the processing of **genetic data** is to evaluate or score of a natural person. [1]
5) **Scoring**. The purpose of data processing is to assess certain characteristics of the data subject, and its result has an effect on the quality or the provision of the service provided and to be provided to the data subject.
6) **Credit rating**. The purpose of data processing is to assess the creditability of the data subject by way of evaluating personal data in large scale or systematically.
7) **Solvency rating**. The purpose of data processing is to assess the solvency of the data subject by way of evaluating personal data in large scale or systematically.
8) **Further use of data collected from third persons**. The purpose of data processing is the use of personal data collected from third persons in the decision to refuse or cancel a service to the data subject.

[1] See the Working Party 29 Guidelines WP248 criteria system's 1st point

9) **The use of the personal data of pupils and students for assessment**. The purpose of data processing—regardless of whether tuition is at primary, secondary or advanced level—is to record and examine the preparedness, achievement, aptitude, and mental state of pupils and students, and the data processing is not statutory.
10) **Profiling**. The purpose of data processing is profiling by way of evaluating personal data in large scale and systematically, especially when it is based on the characteristics of the workplace performance, financial status, health condition, personal preferences or interests, trustworthiness or conduct, residence or movement of the data subject.
11) **Anti-fraud activity**. The purpose of data processing is to use credit reference, anti-money-laundering or anti-terrorism financing, and anti-fraud databases for screening clients.
12) **Smart meters.** The purpose of data processing is the application of 'smart meters' set up by public utilities providers (the monitoring of consumption customs).
13) **Automated decision making producing legal effects** or **similarly significant effects.** The purpose of data processing is to make decisions with legal effects or other significant effects on natural persons, which decisions might result in the exclusion of or discrimination against individuals in certain cases.
14) **Systematic surveillance.** Systematic and large scale surveillance of data subjects in public areas or spaces by camera systems, drones or any other new technology (wifi tracking, Bluetooth tracking or body cameras).
15) **Location data**. Where the processing of location data refers to systematic monitoring or profiling.
16) **Monitoring employee work**. Where the purpose of data processing is the systematic and extensive processing and assessment of employee's personal data in course of the monitoring of employee work, including, e.g. placing GPS trackers in vehicles, and camera surveillance against theft or fraud.[2]
17) **Processing of considerable amounts of special categories of personal data.** Under Recital (91) of the GDPR, processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer.
18) **The processing of considerable amounts of personal data for law enforcement purposes.**
19) Processing of large amounts of data related to **vulnerable data subjects** for purposes different from the original purpose, in the case of, e.g., the elderly, children, and **mentally ill persons.**

[2] See the Working Party 29 Guidelines WP248 criteria system's 1st and 3rd points

20) The processing of the personal data of **children** for profiling, automated decision making, **marketing purposes** or providing them information society related services directly.
21) The use of **new technologies** for data processing. This includes the processing of large amounts of data obtained via sensor-equipped devices (e.g. smart televisions, smart household appliances, smart toys, etc.) and transferred through the Internet or other channels, and such devices providing data on the characteristics of the financial status, health condition, personal interests, trustworthiness or conduct, residence or movement of the natural person, and such data form the basis of profiling.
22) **The processing of health data**. In respect of large amounts of special data processed by hospitals, healthcare providers, and private medical services or non-medical practitioners with a large clientele. This also includes the processing of health data collected from members of major sports establishments or workout rooms.
23) When the data controller is planning to set up **an application**, **tool, or platform for use by an entire sector** to process also special categories of personal data.
24) The purpose of data processing is to **combine** data from various sources for **matching** and **comparison** purposes.

The supervisory authority shall be consulted previously on the result of data protection impact assessment if the data controller—having assessed the risks to the rights and freedoms of data subjects—is unable to bring appropriate measures for reducing risks to an acceptable level, i.e. the residual risks are still high.

Data controllers shall continuously assess the risks arising from their data processing activities in order to recognize when a type of data processing is ‘likely to result in a high risk to the rights and freedoms of natural persons’. The data protection impact assessment is to be a process especially when the data processing operation is dynamic and changes constantly. The data protection impact assessment shall be carried on a necessary basis continuously.