DPIAs "Triggers" – Cheat Sheet

DESCRIPTION

The General Data Protection Regulation ("**GDPR"**) requires organisations processing personal data to be **proactive** with respect to their data-processing activities, by continuously **monitoring** and **evaluating** said activities to ensure they meet the GDPR's principles and requirements.

A key requirement under the GDPR is to undergo a Data Protection Impact Assessment ("**DPIA**"), both as an ongoing need to assess their processing activities' associated risks, and as a result of certain changes or events in an organisation's life cycle. **This is also one of the key responsibilities of the Data Protection Officer of the company**.

The purposes of this document are to:

1. Provide some **practical advice** regarding DPIAs and how to conduct them;

2. Provide some **common and non-exclusive examples on processing operations and areas of application for which a DPIA may be required ("DPIA Triggers").**

WHAT IS A DPIA?

A DPIA is a process aimed at analysing and minimising the data-protection risks inherent within the organisation's business model of processing activities.

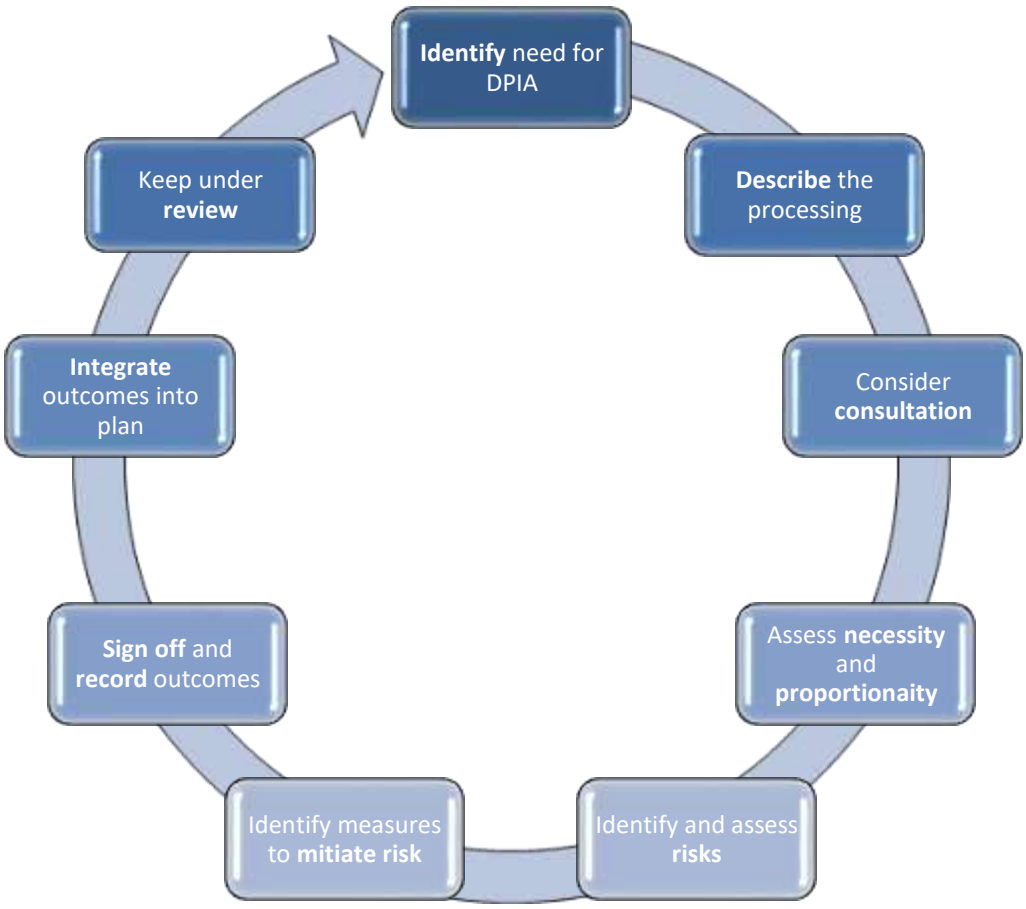
It is a key part of the GDPR's accountability requirements from organisations, and when done properly **helps the organisation to demonstrate its compliance** with data protection regulatory requirements.

HOW DO I CARRY OUT A DPIA?

At a minimum, a DPIA should include:

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks including safeguards, security measures and mechanisms.

A DPIA should begin **early** in the life of a project, **before** processing begins, and **concurrent with the planning and development process**. It should include these steps:



The DPIA process is designed to be flexible and scalable.

You must seek the advice of your Data Protection Officer. You should also consult with individuals and other stakeholders throughout this process.

Note that data protections authorities ("**DPAs**") **recommend publishing your DPIA (or at least its summary)** where possible and after removing sensitive data. Although this is not a requirement under the GDPR, by publishing your DPIA you will be better positioned to foster trust in your processing operations, demonstrating transparency and compliance with the data protection requirements.

DPIA TRIGGERS – WHEN SHOULD I PERFORM A DPIA?

Carrying out a DPIA is **mandatory** in the following scenarios:

1. Where the processing is **likely to result in a high risk** to the rights and freedoms of natural persons;

2. When a **new data processing technology** is being introduced.

In addition, each of the EU's **DPAs have established and published a list of the types of processing operations subject to the requirement of a DPIA**.

Below, you will find common and non-exclusive examples of processing operations and areas of application for which a DPIA may be required.

The below examples should not be taken as definitive or exhaustive, and should **not derogate from the organisation's obligation to assess any processing operation against the requirement to perform DPIAs**.

Generally speaking, **in cases where it is not clear whether a DPIA is required, the regulatory recommendation is that a DPIA should be carried out nonetheless**.

INNOVATIVE TECHNOLOGY

Processing involving the use of new technologies, or the novel application of existing technologies (including AI) when combined with other criteria

- **Artificial intelligence, machine learning and deep learning**
- **Connected and autonomous vehicles**
- **Some IoT applications, depending on the specific circumstances of the processing**
- **Market research involving neuro-measurement (i.e. emotional response analysis and brain activity)**
- **Smart technologies (including wearables)**
- **Intelligent transport systems**

DENIAL OF SERVICE

Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data

- **Credit checks**
- **Mortgage or insurance applications**
- **Other pre-check processes related to contracts (i.e. smartphones)**

LARGE-SCALE PROFILING

Any profiling of individuals on a large scale

- **Data processed by Smart Meters or IoT applications**
- **Hardware/software offering fitness/lifestyle monitoring**
- **Social-media networks**
- **Application of AI to existing process**

DATA MATCHING

Combining, comparing or matching personal data obtained from multiple sources

- **Fraud prevention**
- **Direct marketing**
- **Monitoring personal use/uptake of statutory services or benefits**
- **Federated identity assurance services**

BIOMETRIC DATA

Any processing of biometric data for the purpose of uniquely identifying an individual, when combined with other criteria

- **Facial recognition systems**
- **Workplace access systems/identity verification**
- **Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)**

GENETIC DATA

Any processing of genetic data, other than that processed by an individual genetic professional or health professional for the provision of healthcare direct to the data subject, when combined with other regulatory criteria

- **Medical diagnosis**
- **DNA testing**
- **Medical research**

INVISIBLE PROCESSING

Processing of personal data that has not been obtained directly from the data subject, when combined with any other regulatory criteria

- List brokering
- Direct marketing
- Online advertising
- Online tracking by third parties
- Data aggregation/data aggregation platforms
- Re-use of publicly available data

TRACKING

Processing which involves tracking an individual's behaviour including, but not limited to, the online environment, as well as when involving geolocation data when combined with other criteria

- Social networks, software applications
- Hardware/software offering fitness/lifestyle/health monitoring
- IoT devices, applications and platforms
- Online advertising
- Web and cross-device tracking
- Data aggregation
- Eye tracking
- Data processing at workplace, including processing employees' location data
- Data processing in the context of home and remote working
- Loyalty schemes
- Tracing services (tele-matching, tele-appending)
- Wealth profiling – identification of high-net-worth individuals for direct marketing

TARGETING OF CHILDREN / VULNERABLE INDIVIDUALS FOR MARKETING, PROFILING FOR AUTO DECISION-MAKING, OR THE OFFER OF ONLINE SERVICES

The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.

- **Social networks**
- **Connected toys**

RISK OF PHYSICAL HARM

Where the processing is of a nature such that a personal data breach could jeopardize the health or safety of individuals.

- **Whistleblowing/complaint procedures**
- **Social care records**

HFN'S TECHNOLOGY & REGULATION DEPARTMENT | TEAM LEADERS

- Dr. Nimrod Kozlovski
  Nimrod co-heads HFN's Technology & Regulation Department and is an expert investor in cybersecurity and a teaching professor on Internet and Cyber Law, information technology and innovation. Nimrod earned his doctoral degree in Law (J.S.D) from Yale Law School and conducted his post-doctoral research in Computer Science on Proactive Security at the Yale School of Computer Sciences. Nimrod is also a Partner at JVP, a leading Israeli VC, focusing on Cybersecurity and Big Data, and has formerly founded innovative start-ups.

- Ariel Yosefi
  Ariel co-heads HFN's Technology & Regulation Department and is highly regarded for his global experience advising multinational companies, developers, start-ups and others on regulatory and compliance matters surrounding data protection, cybersecurity and innovative technology compliance.

- Ido Manor
  Ido is a partner in HFN's Technology & Regulation Department, specialising in advising Israeli and international clients, start-ups and internet companies, on a wide range of regulatory and commercial matters involving data protection and privacy, online advertising, user-generated content, social media and mobile marketplaces compliance, e-commerce and international trade.

- Israel (Ruly) Ber
  Ruly is a partner in HFN's Technology & Regulation Department. Ruly joined the department after 8 years as a legal advisor to one of Israel's largest banks. Ruly specialises in advising on data protection and privacy, online advertising, user-generated content, social media and mobile marketplace compliance, as well as financial and banking regulations, and their implications on financial institutions' information and technological procedures.

- Dan Shalev
  Dan is a member of HFN's Technology & Regulation Department, specialising in advising on various technological and regulatory aspects including online advertising and content, intellectual property, data protection and commercial matters. Dan began his legal career at prestigious Israeli law firms and has acquired unique, strategic, relevant experience for advising clients in the fields of online media, ad-tech, content and music production, having acted as VP and COO for two, well-known, ad-tech companies and after co-founding "Bama" Music School and recording studio.