DATA2VAULT
SECURE DATA SERVICES

GDPR: Data Protection Impact Assessment

Since the last data protection directive (EU) of 1995, the way in which data is processed has evolved drastically. Up until more recently individual's rights have not been at the forefront of concern when their data is processed and there has been a divide between individual's rights for protection and the implementation of new technologies. Moreover, the expansion of technology advancements has resulted in data processing becoming more automated. The enforcement of GDPR focuses the protection of individual's rights and attempts to bridge this divide that has been apparent for some time. One of many parts of the GDPR is the requirement to carry out a Data Protection Impact Assessment (DPIA).

What is it, who should be focusing on it and how can it be accomplished?

The Data Protection Impact Assessment (DPIA), also referred to as Privacy Impact Assessment (PIA) is a systematic process to assess the privacy risks to individuals when processing their personal data. Processing involves the collection, use, and disclosure of personal data. This DPIA needs to be undertaken in effort to minimise the risks to the individual and thus is carried out prior to commencing processing by the data controller. GDPR expects the DPIA to be done and the necessary measures implemented to address any risks posed to the individual's privacy through data processing.

This element of the GDPR is the responsibility of the organisations data controller and forms part of the aspect of 'Accountability and privacy by design'. The data controller, being the organisation gathering data.

The regulation is compulsory where a *"type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operation on the protection of personal data".*

Circumstances where this risk may be apparent include:

- Where there is systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. (institutions who conduct automated loan approvals, data analytic providers, online marketing companies and facilities)
- Processing on a large scale of sensitive personal data and personal data relating to criminal convictions and offences. (healthcare providers, insurance companies)
- Large scale systematic monitoring of a publicly accessible areas (the use of CCTV in public areas, leisure areas, restaurants and shopping centres etc.)

Put simply, this means that if the organisation is processing personal data that is likely to result in a high risk to the data subject's rights, a DPIA must be carried out prior to commencing the processing of their personal data.

The DPIA is **NOT** an assessment of the impact on anything else other than personal data protection.

A successful DPIA should ascertain the following outcomes:

- *Whether the data being processed complies with privacy-related legal and regulatory compliance requirements.*
- *The risks and impacts of data processing (in all its forms).*
- *Safeguards and processes for handling information to alleviate any potential privacy risks.*
- *Choices and approaches for individuals to provide consent for the processing of their personal identifiable data.*

A suggested framework to get started

One framework for DPIA does not exist (the GDPR provides a minimum standard for carrying out a DPIA) but organisations should design one that works for them but covers all aspects required by the GDPR.

Following a systematic process can help to tackle the DPIA comprehensively to avoid missing important aspects of the assessment.
In this framework the DPIA process can be portrayed as three stages: Preparation, Evaluation, and Safeguard, Document and Report.

Author: Ricky Magalhaes, Director Managed Security Services

1. **Preparation** (take time to prepare)

In preparation for the DPIA the following actions should be addressed

- The data controller must decide whether there is a legal requirement to carry out the DPIA. This is dependent on the type of data being process as well as the risk to the rights of the individuals
- Once the decision has been made to carry out the DPIA, the goals and scope of the DPIA must be outlined
- The Standard Data Protection Model should be utilised to implement the DPIA to assure compliance is upheld, safeguards identified and, transparency is achieved for the processing system being used.
- The span of the DPIA must be well-defined. An overview of the entire data processing being assessed must be acquired (description of it and purpose for it). Details on the type of data, the format of the data, how and where the data is stored and in what format, how it is transferred, the IT systems and interfaces used. Furthermore, procedures, processes and functional roles utilised.
- Individuals involved and concerned must be identified (All those affected by the use of the data-manufactures, operators, processors, controllers, third parties and individuals)
- Legal requirements need to be recognised –sector specific legal requirements may apply
- A report must be created to document the results for this preparation stage

2. **Evaluation**

This stage comprises the following:

- Identifying protection objectives

The objectives aim to assist with uncovering risk to individuals so that appropriate remedies can be put in place to minimise them. Furthermore, the right balance of the objectives will need to be achieved to suit the persons concerned appropriately and this will be unique to the organisation and the type of data that they process and the systems that they use.

Availability, integrity and confidentiality are three pillars of security and thus form part of the objectives to ensure risk to persons is reduced. Along with these are another three objectives. Together aiming to attain these will support the requirements for protecting the rights of the persons concerned.

1. Availability (to have data accessible and comprehensible when required by authorities)
2. Integrity (data must be reliable-not tampered with or changed and remain accurate)
3. Confidentiality (the need to keep data private)
4. Not linkable (data must not be linked across different domains or used for differing purposes to the intended processing)
5. Transparency (the data subject must be completely aware of how their data is being processed and must give consent)
6. The ability for intervention by the persons concerned (the control that the data subjects have over the data being processed. Can it be made available on request, deleted, blocked or rectified etc.)

- Identification of potential attackers (their motives and objectives)

The DPIA assesses threats from the perspective rights of the persons concerned rather than the threat to the organisation. Thus the aim of the DPIA is to protect the rights of the persons and not the businesses processes of the organisation. The threats must be identified so that they can be safeguarded against.

- Identification of evaluation criteria and benchmarks

Any processing of data impacts the rights of the persons concerned and thus must be justified and assessed under proposed conditions to comply with the regulation. The level of protection must be 'normal' by default but depending on the type of data and types of processing the level can rise to 'high' or 'very high' but never reduced below the 'normal' level.

The protection standards are stipulated as follows:

Normal: no scenarios exist in which the nature of the processing shows potential for a high intensity of interference.

High: special categories of personal data (according to GDPR) are processed and thus a high protection standard is required by law and/or the persons depend on the services/decisions of the organisation.

Very High: Personal data requiring a high protection standard are processed and the person depends on the decisions/services of the organisation. Additionally, there are risks posed by insufficient data security or changes of purposes of processing which the person is unable to become aware of.

- Evaluation of risk

Evaluation of risk is done by making the comparison of the controller's predicted measures or those determined in the progression of the assessment with a catalogue of reference measures formulated and obtainable. If nonconformities occur, they must be assessed on how they might impact the protection objectives (thus increase the risk to the persons concerned) and any insufficiencies in data protection must be rectified accordingly.

3. Safeguard, document and report

- Identify and implement appropriate safeguards

This is dependent on the results of the evaluation and based on the results obtained a plan of risk must be prepared.

The DPIA must have measures to remedy the risks identified and must include safeguards and measures to protect the data. The plan must be unambiguously detailed and include: which safeguards to be taken, who is responsible for implementing the safeguards, the resources available to implement the safeguard, the timeframe for implementation of the safeguard, the criteria to measure the result of safeguards and detail who will evaluate and document the criteria.

- Document and report on the evaluation of results

To achieve the envisioned outcome of the DPIA it is essential to meticulously document and publish a findings report. The report should be standardised to expedite appraisal by authorities, establishments as well as the public.

- Auditing of evaluation results

The DPIA report should be evaluated by an independent third party to ensure it has been properly conducted.

- Review and continuity

The DPIA is not an assessment that is completed once and then forgotten. It is a linear process and must be reviewed and repeated when necessary. If changes in the risks occur, through processing of data, the safeguards must be adapted to reflect the new circumstances and meet the new requirements.

Readiness is key

For a multitude of organisations, the obligatory Data Protection Impact Assessment (DPIA) looms. By May 2018, one of the components to be addressed in order to comply with the GDPR is the DPIA when processing personal data of EU citizens. It is advisable to start outlining a framework and practicing the process as soon as possible as it will take time to iron out any issues and to perfect. Moreover, it is an extremely helpful way to identify risks to the rights of persons concerned so that potential flaws in the data processing systems can be methodically resolved.

Data2Vault Limited
14 Mill Street
Bedford
MK40 3HD

T: 0330 344 2380
W: www.data2vault.com

Author: Ricky Magalhaes, Director Managed Security Services