Data Protection Impact

Assessment Process

Contents

INTRODUCTION **3**

DEFINITIONS 3

DATA PROTECTION IMPACT ASSESSMENT PROCESS **5**

PROCESS DIAGRAM 5

ESTABLISH THE NEED AND CONTEXT 6

DOCUMENT THE USE OF PERSONAL DATA 7

IDENTIFY THE RISKS 8

Identify risk scenarios *8*

ANALYSE THE RISKS 9

Assess the Likelihood *9*

Assess the Impact *10*

Risk Classification *12*

EVALUATE THE RISKS 13

DEFINE RISK TREATMENT PLAN 13

Risk Treatment Options *13*

Selection of Controls *14*

Data Protection Impact Assessment Report *15*

OBTAIN MANAGEMENT APPROVAL FOR RESIDUAL RISKS 15

PRIOR CONSULTATION WITH SUPERVISORY AUTHORITY 16

IMPLEMENT RISK TREATMENT ACTIONS 16

RISK MONITORING AND REPORTING 16

REGULAR REVIEW 17

ROLES AND RESPONSIBILITIES 17

RACI Chart *17*

CONCLUSION 18

Introduction

Tovie AI Limited, hereinafter referred to as the «Company»,is fully committed to protecting the personal data of its customers, employees, suppliers and other stakeholders in accordance with the requirements of the European Union General Data Protection Regulation. We take the privacy of personal data very seriously and have initiated a variety of methods and controls to ensure we know what data we collect and hold and that we protect that data appropriately.

As part of this commitment, Company ensures that all business activities and projects that involve the use of personal data are subject to a data protection impact assessment. The purpose of this assessment is to ensure that our use of personal data is fully understood, that the risks to that data are carefully examined and that all appropriate measures are put in place to protect it throughout its lifecycle.

This document sets out our process for carrying out a data protection impact assessment and, in conjunction with the associated forms and guidance, should be used to ensure that our obligations and policies in this area are met.

Definitions

The following definitions of terms used within this process document are taken from the GDPR:

'personal data'	*means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
'processing'	*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or*

otherwise making available, alignment or combination, restriction, erasure or destruction;

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data Protection Impact Assessment Process

Process Diagram

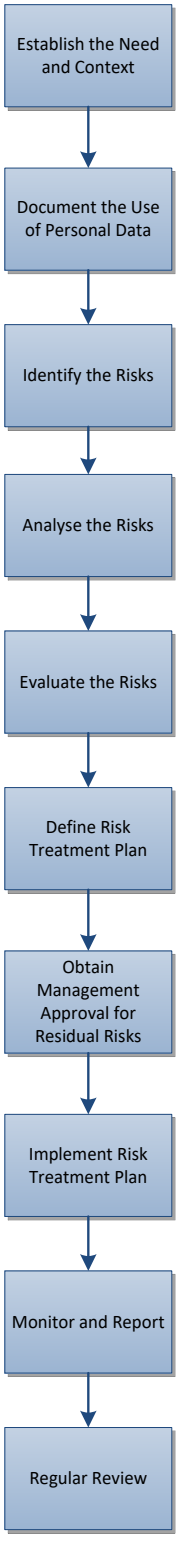

FIGURE 1 – DATA PROTECTION IMPACT ASSESSMENT PROCESS DIAGRAM

Establish the Need and Context

There are a number of criteria that determine when a data protection impact assessment should be carried out within Company. The General Data Protection Regulation (Article 35) specifies that an impact assessment *shall be required* where the proposed processing involves:

- *a 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;*

- *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*

- *a systematic monitoring of a publicly accessible area on a large scale*

Note: Article 9(1) refers to processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

In general, Company specifies that data protection impact assessments are appropriate for projects where one or more of the following applies:

a) information about living individuals will be collected and processed for the first time
b) information about living individuals will be shared with people or organizations that previously did not have access to it
c) change of use of existing personal data
d) the use of new technology that collects or uses data of a personal nature e.g. biometrics

e) existing personal data will be used to reach decisions as part of an automated process
f) it might reasonably be expected that an individual may find any aspect of the project intrusive or the data involved private

If there is uncertainty regarding whether it is appropriate to carry out a data protection impact assessment for a specific project, by default the project team should stay on the side of caution and ensure that one is performed. The Data Protection Officer may be consulted for clarification and further guidance may have been issued by the supervisory authority representing the EU within the country or countries in which the processing will be carried out, in which case this should be consulted also.

The overall environment in which the data protection impact assessment is carried out should be described and the reasons for it explained. This should include a description of the internal and external context of the project and its overall objectives.

The scope of the assessment should also be clearly defined. This may be expressed in terms of the defined scope of the project itself and may include factors such as:

- geographical location e.g. countries, offices, data centres
- organizational units e.g. specific departments
- business process(es)
- IT services, systems and networks
- Customers, products or services

Any specific exclusions to the scope should be stated with reasons.

Document the Use of Personal Data

An appropriate level of detail should be gathered and documented regarding the personal data that is relevant to the project, including:

- Definitions of the specific data items to be stored and processed
- How the data will be obtained
- How the data will be processed
- Retention timescales of the data

- How the data will be stored
- Possible future uses of the data
- Where the data may be transferred to and under what circumstances
- Who will have access to the data and how

This information may be collected and represented in an appropriate combination of information asset registers, flowcharts and via the use of relevant data mapping tools.

Identify the Risks

The process of identifying risks to the personal data we collect, process and hold will consist of the following steps.

Identify risk scenarios

The identification of risks to the identified personal data will be performed by a combination of group discussion and interview with interested parties.

Such interested parties will normally include:

- Manager(s) responsible for each business-critical activity
- Representatives of the people that normally carry out each aspect of the activity
- Providers of the inputs to the activity
- Recipients of the outputs of the activity
- Appropriate third parties with relevant knowledge
- Representatives of those providing supporting services and resources to the activity
- Any other party that is felt to provide useful input to the risk identification process

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk should also be allocated an owner.

Analyse the Risks

Risk analysis within this process involves assigning a numerical value to the a) likelihood and b) impact of a risk. These values are then multiplied to arrive at a classification level of high, medium or low for the risk.

Assess the Likelihood

An estimate of the likelihood of a risk occurring must be made. This should take into account whether it has happened before either to this organization or similar organizations in the same industry or location and whether there exists sufficient motive, opportunity and capability for a threat to be realized.

The likelihood of each risk should be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 1. When assessing the likelihood of a risk, existing controls should be taken into account. This may require an assessment to be made as to the effectiveness of existing controls.

More detailed guidance may be decided for each grade of likelihood, depending on the subject of the risk assessment.

Grade	Description	Summary
1	Improbable	Has never happened before and there is no reason to think it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Likely	On balance, the risk is more likely to happen than not
4	Very Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost certain	Either already happens regularly or there is some reason to believe it is virtually imminent

TABLE 1 - RISK LIKELIHOOD GUIDANCE

The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

Assess the Impact

An estimate of the impact that the risk could have on the organization should be given. This should take into account existing controls that lessen the impact, as long as these controls are seen to be effective.

Consideration should be given to the impact in the following areas:

- Customers
- Finance
- Health and Safety
- Reputation
- Knock-on impact within the organization
- Legal, contractual or organizational obligations

The impact of each risk should be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 2.

More detailed guidance may be defined for each grade of impact, depending on the subject of the risk assessment.

The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

Grade	Description	Customer impact	Financial impact	Health and Safety	Impact on Reputation	Legal impact
1	Negligible	No effect	Very little or none	Very small additional risk	Negligible	No implications
2	Slight	Some local disturbance to normal business operations	Some	Within acceptable limits	Slight	Small risk of not meeting compliance
3	Moderate	Can still deliver product/service with some difficulty	Unwelcome but could be borne	Elevated risk requiring immediate attention	Moderate	In definite danger of operating illegally
4	High	Business is crippled in key areas	Severe effect on income and/or profit	Significant danger to life	High	Operating illegally in some areas
5	Very High	Out of business; no service to customers	Crippling; the organisation will go out of business	Real or strong potential loss of life	Very High	Severe fines and possible imprisonment of staff

TABLE 2 - RISK IMPACT GUIDANCE

Risk Classification

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown in figure 2.

Each risk will be allocated a classification based on its score as follows:

- HIGH – 12 or more
- MEDIUM – 5 to 10 inclusive
- LOW – 1 to 4 inclusive

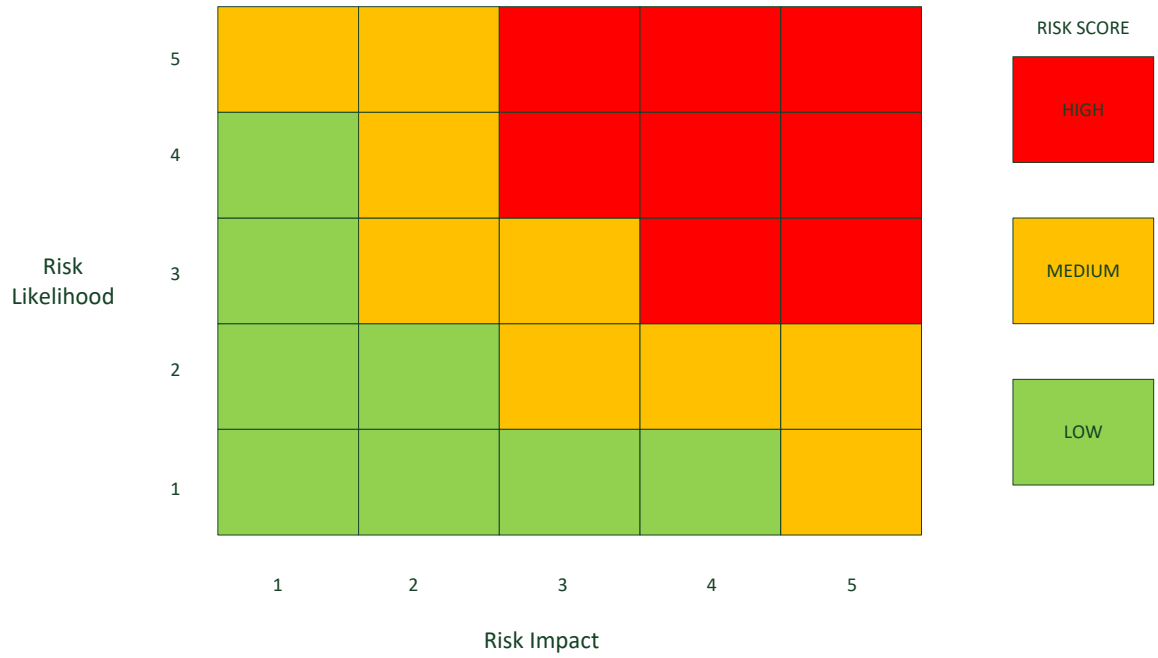

FIGURE 2 - RISK MATRIX CHART

The classification of each risk will be recorded as input to the risk evaluation stage of the process.

Evaluate the Risks

The purpose of risk evaluation is to decide which risks can be accepted and which ones need to be treated. This should take into account the risk acceptance criteria established for this specific risk assessment (see *Risk Acceptance Criteria*, above).

The matrix in *Figure 2* shows the classifications of risk, where green indicates that the risk is below the acceptable threshold. The orange and red areas generally indicate that a risk does not meet the acceptance criteria and so is a candidate for treatment.

Risks will be prioritized for treatment according to their score and classification so that very high scoring risks are recommended to be addressed before those with lower levels of exposure for the organization.

Define Risk Treatment Plan

For those risks that are agreed to be above the threshold for acceptance by Company, the options for treatment will then be explored.

The overall intention of risk treatment is to reduce the classification of a risk to an acceptable level. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g. reducing the score from 8 to 6 means it still remains a medium level risk. Company may decide to accept these risks even though they remain at a medium rating. Such decisions should be recorded with a suitable explanation.

Risk Treatment Options

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

1. ***Modify*** the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk
2. ***Avoid*** the risk by taking action that means it no longer applies

3. ***Share*** the risk with another party e.g. insurer or supplier

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

- Business strategy
- Regulatory and legislative considerations
- Technical issues
- Commercial and contractual issues

DPO will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted, including the risk owner.

Selection of Controls

Appropriate controls will then be identified to reduce either the likelihood or impact (or both) of each risk in order to bring it within acceptable bounds.

In accordance with Company's adoption of the ISO/IEC 27001 standard, Annex A of that document will be used as the starting point for the identification of appropriate controls to address the risk treatment requirements identified as part of the risk assessment exercise. The controls set out in Annex A will be supplemented by the extended and additional guidance set out in the following codes of practice:

- *ISO/IEC 27002 – Code of practice for information security controls*
- *ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- *ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

Data Protection Impact Assessment Report

The evaluation of the treatment options will result in the production of the data protection impact assessment report which will detail:

- A description of the proposed processing operations and the personal data involved
- The purposes of the processing including, where applicable the legitimate interest of the controller of the personal data as defined by the GDPR
- An assessment of the necessity and proportionality of the processing
- The results of the assessment of the risks to the rights and freedoms of the data subjects
- Whether each risk is recommended for acceptance or treatment
- Priority of risks for treatment
- Risk owners
- Recommended treatment option
- Control(s) to be implemented
- Responsibility for the identified actions
- Timescales for actions
- Residual risk levels after the controls have been implemented

Obtain Management Approval for Residual Risks

At each stage of the data protection impact assessment process, management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the data protection impact assessment report and will consider to what extent the report should be made public, either in full or in summarized form.

Signoff will be indicated according to Company documentation standards.

In addition to overall management approval, the acceptance or treatment of each risk should be signed off by the relevant risk owner.

Prior Consultation with Supervisory Authority

In the event that the results of the data protection impact assessment indicate a high level of risk prior to the identified controls being implemented, the GDPR requires that the supervisory authority is consulted before any processing takes place.

The following information must be provided:

- Details of the respective responsibilities of the controller, joint controllers and processors, where applicable
- Purposes and means of the processing
- The controls that will be implemented to protect the data
- Contact details for the data protection officer (if applicable)
- A copy of the impact assessment report

The supervisory authority has eight weeks (extendable by a further six weeks) to provide a judgement on the proposed processing and, if appropriate, give details of what must be done to make the processing acceptable under the GDPR.

Implement Risk Treatment Actions

Once the risk treatment plan has been approved, the necessary actions should be tracked and completed as part of the day to day control of the project. In the event that any actions are delayed or cannot be completed, the implications of this to the protection of the personal data involved must be assessed by management and a decision taken about what to do next. If the untreated risk is sufficiently serious, this may have a significant impact on the viability of the project from a compliance viewpoint and advice should be sought from the Data Protection Officer and/or the supervisory authority in the country or countries affected.

Risk Monitoring and Reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with as part of the management review process.

Regular Review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions or introduction or new or changed IT services.

Roles and Responsibilities

Within the process of risk assessment there are a number of key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown in the RACI table below, together with their relative responsibilities at each stage of the process.

RACI Chart

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

R= Responsible A= Accountable C= Consulted I= Informed

Role: / Step	Assessment Lead	Risk owners	Top management
Establish the need and context	**R**	**C**	**A**
Document the use of personal data	**R**	**C**	**A**
Identify the risks	**C**	**R**	**A**
Analyse the risks	**C**	**R**	**A**

Evaluate the risks	**C**	**R**	**A**
Define risk treatment plan	**R**	**C**	**A**
Management approval for residual risks	**C**	**C**	**A/R**
Implement risk treatment plan	**R**	**R**	**A/R**
Monitor and Report	**R**	**I**	**A**
Regular Review	**R**	**C**	**A**

TABLE 3 - RACI CHART

Further roles and responsibilities may be added to the above table as the data protection impact assessment process matures within Company.

Conclusion

The process of data protection impact assessment is fundamental to the implementation of a successful project that handles personal data and is a significant part of the GDPR legislation. Only by fully understanding its risks with regard to personal data can an organization hope to ensure that the controls it has in place are sufficient to provide an appropriate level of privacy and meet the high standard expected of it.

For a cloud service provider, the regular assessment of risks to personal data and the application of comprehensive controls is vital to the continuing confidence of its cloud service customers and in meeting its obligations to protect personal data from all too common threats.

By following this process Company will go some way to ensuring that the risks that it faces in the day-to-day operation of its business are effectively managed and controlled.