Privacy Impact Assessment Worksheet

Scenario:

You are working for the independent game studio *Derivative Games* and are on the planning team for their new game *Diavolo 3*.

Although the studio is profitable this will be the largest project they have released. Management expects sales of the game to increase the company’s annual turnover to over $3 million.

The owner and founder would like to use the existing customer database to send marketing material directly to customers via email. This has raised some concern amongst the team as the company does not have an existing ‘opt-in’ mailing list (although it does have customer email addresses stored in their customer database), or a policy on direct marketing.

The company would also like to start taking pre-orders for the game once development has reached the *beta* milestone, which is scheduled for 3 months from now. This will require the collection of personal information and payment from customers. You will need to ensure that this information is stored securely so that all customers receive their orders once the game is released.

You have found the existing privacy policy for *Derivative Games*, but you’re not sure if this adequately informs customers of how their data is used, or if it will cover how your team would like to use customers’ personal information for this project.

Complete this worksheet with reference to the scenario above.

Privacy Impact Assessment:

Answer the following questions to complete the privacy impact assessment for the project described in the scenario.

## Threshold assessment

*a) Will any personal information be collected, stored, used or disclosed as part of your project?*

Remember that personal information does not always have to include details such as an individual’s name to qualify as personal information.

|  |
| --- |
|  |

*b) If yes, record the different types of personal information that will be handled.*

|  |
| --- |
|  |

*c) If no, record the reasons for your decision*

|  |
| --- |
|  |

## Describe

*Write a brief description of your project*

|  |
| --- |
|  |

## Identify and consult with stakeholders

*List the stakeholders for your project, and indicate whether you will consult with all stakeholders, or undertake a targeted consultation*

**Internal**

|  |
| --- |
|  |

**External**

|  |
| --- |
|  |

## Map information flows

*Draw a diagram that outlines the information flows in your project*(You can refer to the lecture or this site if you need guidance: <https://education.oaic.gov.au/elearning/pia/topic4.html>)

## Privacy impact analysis and compliance check

*a) List some of the positive privacy impacts of your project*

|  |
| --- |
|  |

*b) List some of the negative privacy impacts of your project*

|  |
| --- |
|  |

*c) Does your project comply with the APPs?*

Remember to make a record of whether the APP is relevant to your project, whether your project complies, and whether there are any risks to compliance. You may also wish to consider likely community perceptions and expectations in relation to each APP.

(If the scenario does not have enough information for you to determine if the project is compliant with one or more APPs, write what the company could do to become compliant)

**APP 1 — open and transparent management of personal information**

|  |
| --- |
| No – privacy policy not up to date |

**APP 2 — anonymity and pseudonymity**

|  |
| --- |
|  |

**APP 3 — collection of solicited personal information**

|  |
| --- |
|  |

**APP 4 — dealing with unsolicited personal information**

|  |
| --- |
|  |

**APP 5 — notification of the collection of personal information**

|  |
| --- |
|  |

**APP 6 — use or disclosure of personal information**

|  |
| --- |
|  |

**APP 7 — direct marketing**

|  |
| --- |
|  |

**APP 8 — cross-border disclosure of personal information**

|  |
| --- |
|  |

**APP 9 — adoption, use or disclosure of government related identifiers**

|  |
| --- |
|  |

**APP 10 — quality of personal information**

|  |
| --- |
|  |

**APP 11 — security of personal information**

|  |
| --- |
|  |

**APP 12 — access to personal information**

|  |
| --- |
|  |

**APP 13 — correction of personal information**

|  |
| --- |
|  |

## Privacy management — addressing risks

List the risks to privacy that you identified in your privacy impact analysis and compliance check (the section above).   
For each risk, list three options to remove, minimise or mitigate these privacy risks.   
  
(Feel free to add more risks if needed)

|  |
| --- |
| **Privacy risk** |
| No transparent handling of personal information |
| *Mitigation strategies* |
| * Update privacy policy * Inform customers of updated policy and how they can get more information on how their data is used * Create procedure to conduct regular (yearly) reviews of the privacy policy |

|  |
| --- |
| **Privacy risk** |
|  |
| *Mitigation strategies* |
|  |

|  |
| --- |
| **Privacy risk** |
|  |
| *Mitigation strategies* |
|  |

## Recommendation

Consider the mitigation strategies you have listed above. Outline:

* + - * which mitigation strategy you recommend your organisation adopts to address each privacy risk
      * the individual or business area responsible for carrying out the recommended action
      * your suggested timeframe for implementation

|  |
| --- |
|  |