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.

|  |
| --- |
| Yes |

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

|  |
| --- |
| Customer email addresses  Payment method details, e.g., Billing address, Shipping address, Credit/Debit card information |

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

|  |
| --- |
| N/A |

## Describe

*Write a brief description of your project*

|  |
| --- |
| The creation of Diavolo 3, an action packed, fast paced video game that tells the emotional and compelling story of a serial murderer. |

## 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**

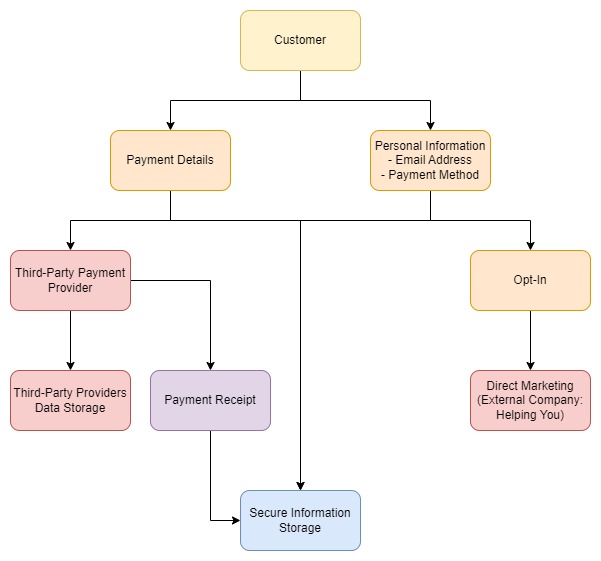
|  |
| --- |
| Project manager  Marketing team  Owner  Founder  Dev Team  Will consult internal stakeholders as they are directly involved in the development and marketing of the game. They provide valuable information in their areas. |

**External**

|  |
| --- |
| Sponsors  Lawyers  Customers  Government Regulator  Publisher  Third-Party payment providers  Selected and relevant external stakeholders will be consulted. The company will consult our third-party payment providers to ensure they are handling customer information correctly. |

## 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*

|  |
| --- |
| Privacy Policy clearly states the current use of customer information, |

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

|  |
| --- |
| Does not have an opt-in mailing list, Privacy policy needs to be updated |

*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**

|  |
| --- |
| Relevance: Yes  Compliant: No  Reasoning: Privacy Policy is not updated |

**APP 2 — anonymity and pseudonymity**

|  |
| --- |
| Relevance: No, company requires personal information to process pre-orders |

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

|  |
| --- |
| Relevance: Yes  Compliant: Partial  Reasoning: Opt-In and Opt-Out is planned to be implemented for collection of email addresses |

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

|  |
| --- |
| Relevance: No  Compliant: Yes  Reasoning: Only necessary information is collected for the purpose of pre-ordering and direct-marketing. and all of which is solicited, any unsolicited personal information is not collected or used. |

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

|  |
| --- |
| Relevance: Yes  Compliant: No  Reasoning: No current notification to customer that their information will be collected, however Opt-In can include a disclaimer that their date will be collected for the purpose of marketing |

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

|  |
| --- |
| Relevance: Yes  Compliant: Partial  Reasoning: Currently customers are not completely informed as to how their data will be collected, used or shared to third-party companies. This could be added to the privacy policy and a disclaimer to the Opt-In to recieve marketing. |

**APP 7 — direct marketing**

|  |
| --- |
| Relevance: Yes  Compliant: Partial  Reasoning: Privacy Policy is to be updated to explain how personal information is used for marketing as well as a disclaimer to the opt-in explaining how their information will be used for direct marketing. |

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

|  |
| --- |
| Relevance: Yes  Compliant: No  Reasoning: Privacy Policy is not updated to explain that information will be shared to the third-party marketing company *Helping You* an overseas company situated in the United States. |

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

|  |
| --- |
| Relevance: No  Compliant: Yes  Reasoning: No government related Identifiers are collected |

**APP 10 — quality of personal information**

|  |
| --- |
| Relevance: Yes  Compliant: Partial  Reasoning: No way for customers to access or update their personal information, to ensure accuracy of emails collected, a simple verification email could be used. |

**APP 11 — security of personal information**

|  |
| --- |
| Relevance: Yes  Compliant: Partial/Unclear  Reasoning: Current security of Customer Database is unclear, however a password protected database with limited access for selected authorised personnel would make company compliant. |

**APP 12 — access to personal information**

|  |
| --- |
| Relevance: Yes  Compliant: Partial/Yes  Reasoning: Company could make accessing this information easier |

**APP 13 — correction of personal information**

|  |
| --- |
| Relevance: Yes  Compliant: Partial  Reasoning: Collected data is correct, but option for customers to access and update their information would make company more compliant. |

## 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** |
| Company doesn’t notify or inform customers how their information will be used for marketing |
| *Mitigation strategies* |
| * Update privacy policy to inform customers how their information will be used for marketing * Add a disclaimer to Opt-In for direct marketing * Upon pre-order customers are notified how their information may be used for direct marketing |

|  |
| --- |
| **Privacy risk** |
| Inadequate security measures for storing and processing personal information |
| *Mitigation strategies* |
| * Require employees to use strong passwords and follow strong security protocols (i.e., do not share passwords) * Regularly review and update security measures to ensure they are up to date. * Ensure antimalware software is up to date to minimise risk to working on computers |

## 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

|  |
| --- |
| **No transparent handling of personal information**  Mitigation strategy: *Update privacy policy to inform customers how their information will be used for marketing*  Responsible Party: *Administration*  Timeframe: *2 months (before launch of beta and pre-orders)*  **Company doesn’t notify or inform customers how their information will be used for marketing**  Mitigation strategy: *Add a disclaimer to Opt-In for direct marketing and update privacy policy*  Responsible Party: *Administration*  Timeframe: *2 months (before launch of beta and pre-orders)*  **Inadequate security measures for storing and processing personal information**  Mitigation strategy: *Regularly review and update security measures to ensure they are up to date.*  Responsible Party: *Administration*  Timeframe: *On a regular basis, at least once a year, preferably more often* |