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  Customer personal information: billing address, shipping address, payment address |

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

|  |
| --- |
|  |

## Describe

*Write a brief description of your project*

|  |
| --- |
| Diavolo 3 is an action-packed RPG game developed by Derivative Games, set in several different big cities filled with crime and destruction |

## 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  Dev Team  Founder  Will consult internal stakeholders as they are directly involved in the development and marketing of the game. They provide valuable information on their respective areas |

**External**

|  |
| --- |
| Investors  Lawyers  Customers  Government Regulator  Third party payment providers  Selected 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>)

Diagram

Description automatically generated with low confidence

## Privacy impact analysis and compliance check

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

|  |
| --- |
| * Privacy Policy Review: |

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

|  |
| --- |
| * Does not have a Opt-In mailing list; |

*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: relevant  Compliance: no  We are not compliant |

**APP 2 — anonymity and pseudonymity**

|  |
| --- |
| Not relevant, the company requires personal info in order to process pre-orders. |

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

|  |
| --- |
| Partially, Opt-in is currently planned to be implanted in the future. |

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

|  |
| --- |
| Not relevant, company only collects personal information that is necessary for the purpose of processing pre-orders or for the direct marketing strategy. |

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

|  |
| --- |
| Is relevant and currently not complied. Thye company has not notified customers about the collection of their personal information. The Opt-in can include this disclaimer for future customers. |

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

|  |
| --- |
| Relevant and partially compliant, currently haven’t notified customers on how their information will be used for marketing purposes. The company can notify customers about the collection of their personal data for the use of marketing. |

**APP 7 — direct marketing**

|  |
| --- |
| Relevant and partially compliant, company needs to implement opt-in for the ise of information for direct marketing. |

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

|  |
| --- |
| Not relevant, as the company doesn’t disclose personal information to overseas entities |

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

|  |
| --- |
| Not relevant, as the company does not gather government related identifiers. |

**APP 10 — quality of personal information**

|  |
| --- |
| Relevant, and compliant. The company could also prompt users to update their information when making a purchase. |

**APP 11 — security of personal information**

|  |
| --- |
| Relevant, partial/unclear. It is important to store their date and customer personal information securely  Failure to competently store customer data, would reflect poorly and damage the brand’s reputation |

**APP 12 — access to personal information**

|  |
| --- |
| Relevant, compliant. Company can make accessing this information easier users. |

**APP 13 — correction of personal information**

|  |
| --- |
| Relevant and compliant. Company could offer the ability for the user to edit their 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** |
| Company doesn’t notify customers on how their information will be used |
| *Mitigation strategies* |
| * Opt-in marketing can include a disclaimer for how the information will be used * Update privacy policy to clarify how customer information is used * Upon pre-order. Customers are notified about how their billing information will be used to fulfill the pre-order. |

|  |
| --- |
| **Privacy risk** |
| Inadequate security measures for storing and processing personal information |
| *Mitigation strategies* |
| * Require employees to use stronger passwords, and use stronger security protocols. * Regularly review and update security measures to ensure they maintain effective. * Up to date anti-malware software to minimize risk of working 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

|  |
| --- |
| * Company doesn’t notify customers on how their information will be used Mitigation Strategy: * Update privacy policy to clarify how customer information is used * Responsible Party: Administration * Timeframe: 2 months * Opening unknown websites and links * Scan computer to clarify if it have been compromised and people are able to see and steal private/unreleased information * Responsible Party : Admin * Timeframe: 2 months |