Workplace Information Handling Workbook

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.

With reference to the scenario above, answer the following questions (answer in the boxes provided):

Question 1:

In Australia, what piece of legislation regulates the way individuals’ personal information is handled?

|  |
| --- |
| Privacy Act 1988 |

Question 2:

Within the legislation from Question 1, there are 13 principles. Collectively, what are these principles called?

|  |
| --- |
| Australian Privacy Principlesy |

Question 3:

Based on the information you have, will *Derivative Games* need to comply with this legislation? Why?

|  |
| --- |
| Yes, Derivative games will have a turnover of more then 3 million a year |

Question 4:

For the purposes of this project, we will classify workplace data using three types: non-sensitive data, proprietary information, and personal information.

*Proprietary information*: information that the company wishes to keep secret. This may include business strategy, employment contracts, game designs, source code, and similar information.

*Personal information*: any personally identifiable information, whether this belongs to customers, business partners and contractors, or direct employees.

*Non-sensitive information*: publicly available data and other data not included in the definition of personal information or proprietary information.

Identify as many types of workplace data as you can from the scenario and classify them according to these three data types. (You may speculate about the information various teams within the company may need to work with for the project described in the scenario – for example, the source code the developers work on for *Diavolo 3* would be classified as proprietary information).

Try to list 2 pieces of information for each type. You may wish to discuss this with your group or class.

|  |  |  |
| --- | --- | --- |
| Non-Sensitive Information | Proprietary Information | Personal Information |
| Date of Birth  Name | - project source code |  |

Question 5:

List all personally identifiable information that you think *Derivative Games* will need to collect for this project. (Aim for at least 2 items. The first one has been provided for you)

As you list each piece of PII, consider whether it is actually necessary to collect and hold that personal information in order to carry out your functions and activities. (Over-collection can increase risks for the security of personal information).

|  |  |
| --- | --- |
| Business Use | Personal Information Collected |
| e-mail mailing list | e-mail address |
| Beta Testers | Player account ID |
| Pre-Orders | Customer personal information: Billing address, shipping address, payment details |
|  |  |
|  |  |
|  |  |

Question 6:

For each piece of personal information collected, plan how the personal information will be handled.

List how the personal information will be stored and who will have access to it.

Consider how privacy protections can be embedded into the handling process, or how existing privacy protections could be strengthened.

You may wish to discuss this question with your team or class.

|  |  |
| --- | --- |
| PII Collected | Handling Process |
| e-mail address | e-mail addresses collected via web form and automatically stored in a company owned database Access to the database can be controlled with a password |
| Player account id | Player account ID collected via player signing up for the game beta test, and automatically stored in a company database. Access to the database is regulated with a password, only accessible by required individuals. |
|  |  |
|  |  |
|  |  |
|  |  |

Question 7:

Review *Derivative Game’s* privacy policy.

In your opinion, does the existing policy adequately inform customers about how their personal information could be used?

|  |
| --- |
| no |

If no, identify the areas where the policy would need to be modified. You may wish to discuss this with your team or class.

|  |
| --- |
| They do not mention the use of private information for marketing purposes, and there is no visible “opt-out” option for users.  The policy would also need to ensure it cover the organization’s responsibility to comply with an opt-out request & provide the user request, the source for the individual’s private information. |

Question 8:

Your team is considering using an external marketing company, *Helping You*, to conduct marketing activities on behalf of *Derivative Games*. *Derivative Games* would need to give *Helping You* access to some personal information of customers, like names and email addresses. This company is based the US.

Which of the 13 principles from Question 2 would *Derivative Games* need to consider, and why?

|  |
| --- |
| APP 1: Ensure they are transparent on how they use the data  APP 5: Wither the personal information is likey to be disclosed to overseas recipients  APP 6: Personal information con only be used or disclosed for purposes it was collected for (unless has consented for other purposes)  APP 8:  Cross-border disclosed for personal information |

Question 9:

Review the lesson on *Data Integrity Threats*.

What are three common threats to data integrity?

|  |
| --- |
| Poor Passwords |
| Improper security networks |
| Expired software and applications |

What are some ways the company could minimise these threats?

|  |
| --- |
| Poor Passwords – using different passwords for all accounts, 2fa, re-enter passwords after 30 days  Improper networks – banning sites,  Expired software – keep up to date with subscriptions |