

Appendix C: SDL Privacy Questionnaire

Article 05/22/2012

This sample document provides some criteria to consider when you build a privacy questionnaire. It is not an exhaustive list, and should not be treated as one.

On This Page

Introduction

Identify Your Project and Key Privacy Contacts

Initial Assessment

Determine Your Privacy Impact Rating

Understand Your Obligations and Try to Lower Your Risk (for P1 and P2 scenarios)

Identify a Compliant Design

Perform a Detailed Privacy Analysis for P1 scenarios

Conduct a Design Review with Your Privacy Advisor

Test Your Privacy Experience

Create a Draft Privacy Disclosure

Designate Your Privacy Incident Response Contact

Obtain Approval from Your Privacy Advisor

Introduction

The following questions are designed to help you complete the privacy aspects of the Security Development Lifecycle (SDL). You will complete some sections, such as the initial assessment and a detailed analysis, on your own. You should complete other sections, such as the privacy review, together with your privacy advisor.

Identify Your Project and Key Privacy Contacts

- What is the name of your project?


- When will the public first have access to this project?

- Who on your team is responsible for privacy?

Initial Assessment

The initial assessment is a quick way to determine your *Privacy Impact Rating* and to estimate the work required to be compliant. The rating (P1, P2, or P3) represents the degree of risk your software presents from a privacy perspective. You need to complete only the steps that apply to your rating. For more detail, see the main Microsoft [Security Development Lifecycle document](#).

Determine Your Privacy Impact Rating

Check all behaviors that apply to your software. If your software does not exhibit any of the behaviors, check "None of the above." For more information, see the [Privacy Guidelines for Developing Software Products and Services](#) .

☐ Stores personally identifiable information (PII) on the user's computer or transfers it from the user's computer (P1)

☐ Provides an experience that targets children or is attractive to children (P1)


☐ Continuously monitors the user (P1)

☐ Installs new software or changes file type associations, home page, or search page (P1)


☐ Transfers anonymous data (P2)

☐ None of the above (P3)

Understand Your Obligations and Try to Lower Your Risk (for P1 and P2 scenarios)

Before you invest time in a design or implementation, get a feel for the work it will take and investigate ways to lower your overall privacy risk. Higher risk translates to higher development and support cost. For more information, see the [Privacy Guidelines for Developing Software Products and Services](#) .

Identify a Compliant Design

For more information, see the [Privacy Guidelines for Developing Software Products and Services](#) .

Perform a Detailed Privacy Analysis for P1 scenarios

Before your privacy design review, analyze your threat model to identify any PII that you store or transfer. Summarize the privacy aspects of your software in a detailed analysis.

- Describe the PII you store or data you transfer:

- Describe your compelling user value proposition and business justification:

- Describe any software you install or changes you make to file types, home page, or search page:

- Describe your notice and consent experiences:

- Describe how users will access your public disclosure:

- Describe how organizations can control your feature:


- Describe how users can control your feature:

- Describe how you will prevent unauthorized access to PII:

Conduct a Design Review with Your Privacy Advisor

To avoid costly mistakes, projects with an impact rating of P1 must hold a design review with a privacy advisor before investing heavily in implementation.

Test Your Privacy Experience

Verify that your software complies with privacy requirements. For more information about privacy criteria, see the [Privacy Guidelines for Developing Software Products and Services](#) .

Create a Draft Privacy Disclosure

Work with your privacy advisor to write and post a privacy disclosure.

Designate Your Privacy Incident Response Contact

If your software is involved in a privacy incident, your team must be prepared to follow the [Privacy Escalation Response Framework \(Appendix K\)](#).

Who on your team is the primary contact for Privacy Incident Response?

Obtain Approval from Your Privacy Advisor

Before you ship your project externally, you must obtain approval from your privacy advisor.

Content Disclaimer

This documentation is not an exhaustive reference on the SDL process as practiced at Microsoft. Additional assurance work may be performed by product teams (but not necessarily documented) at their discretion. As a result, this example should not be considered as the exact process that Microsoft follows to secure all products.

This documentation is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This documentation does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft Corporation. All rights reserved.

Licensed under [Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported](#) 