PERCEPTUAL COMPUTING SOFTWARE DEVELOPMENT KIT ("SDK")

PRE-RELEASE LICENSE AGREEMENT

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.

DO NOT USE OR LOAD THIS SOFTWARE (THE "SOFTWARE") UNTIL YOU HAVE CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY LOADING OR USING THIS INTEL SOFTWARE, YOU AGREE TO THE TERMS OF THIS SOFTWARE DEVELOPMENT KIT LICENSE AGREEMENT (THIS "AGREEMENT"). IF YOU DO NOT WISH TO SO AGREE, DO NOT COPY, INSTALL OR USE THIS INTEL SOFTWARE. IF YOU ARE AN AGENT OR EMPLOYEE OF A LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND SUCH LEGAL ENTITY TO THIS AGREEMENT.

NOTICE:

1. All Applications and Components developed using this Software must comply with Intel's privacy, security, content and other validation criteria set forth in Exhibit A, which may be updated from time to time. In addition, the Software is deemed to be pre-release code (e.g., alpha or beta release, etc), which may not be fully functional and which Intel or its licensors may substantially modify in development of a commercial version. Neither Intel nor such licensors makes any assurances that they will ever develop or make generally available a commercial version of any such Software. You agree to maintain as confidential all information relating to your use of the Software and not to disclose to any third party the Software and/or any benchmarks, performance results, or other information relating to the Software.

2. Definitions: In this Agreement, the following capitalized terms shall have the meanings below:

a. **"Application"** means a software application and all materials related to such application designed for use on an Intel-branded processor based computing system.

b. **"Component"** means a reusable module that can be incorporated into other applications in the form of middleware, libraries, modules, etc. that may be submitted by other developers, designed for use on an Intel-branded processor based computing system.

c. **"Purpose"** means your internal evaluation and review solely to advise Intel as to possible modifications or enhancements to the Software or to evaluate the desirability of cooperating with Intel in developing Applications and/or Components based upon the Software. You may not externally disclose, externally distribute or make any commercial use whatsoever of the Software, including as part of or with your Application and/or Component.

3. LICENSE.

3.1 Subject to the restrictions in Section 3.3, Intel Corporation ("Intel") grants to you the following

non-exclusive, non-transferable, non-assignable, royalty-free licenses (i) under its copyrights in the Intel-developed portions of the Software and (ii) under third party licensors' copyrights for their respective applications that may be included in the Software, a sublicense in such third party licensors' respective portions of the Software, (and as applicable pursuant to Section 3.2 below): to design, develop, debug or otherwise create or modify Applications, Components or other software products, in each case, solely in connection with the Purpose, subject to the following:

- **Developer Tools** include libraries, developer documentation, installation or development utilities, and other materials. You may use and distribute the foregoing items internally for the purposes of using the Software as licensed hereunder, but you may not externally redistribute them.

- **Sample Source** may include example interface or application source code. You may copy, modify and compile the Sample Source and include it in your Application and/or Component in binary and source code form solely for the Purpose. You may not externally distribute the Sample Source in any form, including as part of or with your Application and/or Component.

- **End-User Documentation** includes textual materials intended for end users. You may internally copy and use them solely for the Purpose, but you may not externally distribute such materials.

- **Licensed Binaries** are code provided in binary form. You may internally copy and use the Licensed Binaries solely for the Purpose. You may not externally distribute the Licensed Binaries in any form, including as part of or with your Application and/or Component.

- **Header Files** are source files for use by you for the purposes of using the Software as licensed hereunder, but you may not externally redistribute them as part of or with your Application and/or Component.

3.2 Notwithstanding Section 3.1 above, the Software may contain certain open source software, identified in, and licensed in accordance with, the "license.txt" file or other text or file in the Software.

3.3 **Restrictions.** Your use of the Software is expressly limited to and conditioned upon compliance with the

following:

- You will not alter, remove or obscure any proprietary notices from the Software relating to Intel's or Intel's licensors' intellectual property rights.

- You will make reasonable efforts to discontinue use of the portions of the Software that you are licensed hereunder to use, upon Intel's release of an update, upgrade or new version of the Software.

- You may not reverse-assemble, reverse-compile, or otherwise reverse-engineer any portion of the Software provided solely in binary form.

- You must not disable or by-pass any security features of the Software, or use the Software to develop Applications or Components that (i) can disable or by-pass such security features or (ii) can cause a Security Vulnerability. "Security Vulnerability" means a weakness or flaw in a product or system's design, operation or implementation that could be exploited by an attacker to violate the product or system's security or privacy policies, including without limitation, a flaw that makes it infeasible, even when the product is properly used, to prevent an attacker from usurping privileges on a user's

system, compromising its data, security or other operational features. If you become aware that your Applications or Components can cause a Security Vulnerability, you agree to (1) immediately notify Intel, (2) take immediate measures to stop the internal distribution of your Applications or Components, (3) promptly correct such Security Vulnerability and (4) indemnify Intel for any claims that may be alleged against Intel due to such Security Vulnerability.

- You may not externally distribute any portion of the Software, including as part of or with your Application and/or Component.

4. OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its licensors. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel or its licensors may make changes to the Software, or to items referenced therein, at any time without notice, but neither are obligated to support or update the Software. Except as otherwise expressly provided, neither Intel nor its licensors grant any express or implied right under Intel or Intel's licensors patents, copyrights, trademarks, or other intellectual property rights.

5. FEEDBACK. This Agreement does NOT obligate you to provide Intel with comments or suggestions regarding the Software. However, should you provide Intel with comments or suggestions for the modification, correction, improvement or enhancement of (a) the Software or (b) products or processes which work or interact with the Software, you grant to Intel and/or Intel's licensors (where your comments or suggestions relate to their respective applications that may be included in the Software) a non-exclusive, irrevocable, worldwide, royalty-free license, with the right to sublicense Intel's licensees and customers and/or Intel's licensors' licensees and customers, under your intellectual property rights, the rights to use and disclose such comments and suggestions in any manner Intel and/or Intel's licensors choose and to display, perform, copy, make, have made, use, sell, and otherwise dispose of Intel's and Intel's licensors' and their sublicensee's products embodying such comments and suggestions in any manner and via any media Intel and/or Intel's licensors choose, without reference to the source.

6. EXCLUSION OF WARRANTIES. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR

FITNESS FOR A PARTICULAR PURPOSE. Neither Intel nor its licensors provide any warranty or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

7. LIMITATION OF LIABILITY. IN NO EVENT SHALL INTEL OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST DATA, LOSS OF GOODWILL, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. THE SOFTWARE LICENSED HEREUNDER IS NOT DESIGNED OR INTENDED FOR USE IN ANY MEDICAL, LIFE SAVING OR LIFE SUSTAINING SYSTEMS, TRANSPORTATION SYSTEMS, NUCLEAR SYSTEMS, OR FOR ANY OTHER MISSION CRITICAL APPLICATION IN WHICH THE FAILURE OF THE SOFTWARE COULD LEAD TO PERSONAL INJURY OR DEATH OR FOR USE IN ANY SECURITY-RELATED USE CASES. THE WARRANTY DISCLAIMER AND LIMITED LIABILITY ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN INTEL, ITS LICENSORS AND YOU. INTEL AND ITS LICENSORS WOULD NOT BE ABLE TO PROVIDE THE SOFTWARE WITHOUT SUCH LIMITATIONS.

8. TERMINATION OF THIS AGREEMENT. This Agreement will terminate without notice on the last day of the pre-release period, which may be specified by Intel, or if not specified, upon the commercial release of the Software by Intel. Intel may terminate this Agreement immediately at any time if you violate its terms and such breach is not cured within thirty (30) days of written notice from Intel. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

9. APPLICABLE LAWS. Claims arising under this Agreement shall be governed by the laws of Delaware, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. Neither Intel nor its licensors are obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

10. TRADE COMPLIANCE. You and or any of your subsidiaries shall not import, export, reexport, distribute or transfer either directly or indirectly, any product, service or technical data or system incorporating such items without first obtaining any required license or other approval from the U.S. and any other worldwide government agency that has jurisdiction over such trade activities.

11. ASSIGNMENT. Intel may assign its rights or delegate its obligations, or any part thereof under this Agreement without prior consent from you. You may not assign, whether in conjunction with a change of ownership, merger, acquisition, sale or transfer of all, substantially all or any part of your business or assets or otherwise, either voluntarily, by operation of law of otherwise, any portion of this Agreement. Any attempt by you to assign or delegate any rights, duties or obligations set forth in this Agreement without Intel's prior written consent shall be deemed a material breach of this Agreement and shall be null and void. Except as provided above, the terms and conditions of this Agreement shall bind and inure to each party's successors and assigns.

12. AMENDMENTS. Intel may make changes to this Agreement at any time by sending You a notice to the e-mail address on record describing the modifications made. Intel will also endeavor to post a notification on the Intel's website where you can download the Software describing the modifications made. The changes will become effective, and will be deemed accepted by You, (a) immediately for those who download the Software after the notification is posted, and (b) for pre-existing users, upon acceptance of the modified Agreement (except changes required by law which will be effective immediately). If You are a pre-existing user and you do not accept the updates to this Agreement, Intel may suspend or terminate this Agreement. If You do not accept updates to this Agreement, Your sole and exclusive remedy shall be to cease use of the Software.

GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or its successor. Use of the Software by the Government constitutes acknowledgment of Intel's proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052.

EXHIBIT A

Privacy Requirements and Recommendations for Development using the Intel® Software Development Kit: What Developers Should Know

Disclaimer: Nothing in this document should be interpreted as legal advice.

Purpose

The purpose of this document is to acquaint the developer ("you") with Intel's privacy philosophy and how privacy and security controls can be easily incorporated into your exploration, planning, and development efforts. The intention is to briefly define the must have requirements as well as describe recommendations based on Fair Information Practices Principles[1] and offer additional reading resources for more information. This document will help prepare you to proactively design your application to protect and respect customers' privacy interests.

You should be aware that compliance with international privacy standards and regulations can be complicated and includes legal risks. If the application or business objective does not require processing personal information from the user, the best practice is not to process such information.

1. Privacy Requirements

Intel may require You to stop any distribution of Applications not meeting these requirements. Any user complaints related to personal information misuse may be considered as grounds for termination of the Software license by Intel.

1.1. Notice to users - If your application collects or uses any personal information, the user must be notified about what is being collected/used, why it is being collected/used (purpose) and whether the information will be shared with anyone else.

1.1.1. Implementation Example: Provide brief description of your privacy notice with a link to more detailed information.

1.1.2. Definitions of personal information may vary in different countries. Developers should use a very broad interpretation of this term to include any information that is directly or may be associated with a person. Examples can include: Images, voice, location, name, address, birthday, gender, logged activities, survey responses, etc.

1.2. Use limitation - Personal information may only be used for the purpose described in the notice.

1.3. Explicit opt-in for transfer to third parties - If you share any collected personal information with third parties, you must obtain the user's permission before the information is transferred.

1.3.1. Implementation Example: Identify the third party, the information to be shared and the purpose for sharing the information before asking for user consent. Consent should not be sought for "blanket" approval to share with "any" third parties for "any legal" purpose.

1.3.2. Implementation Example: In a social media context, users may have active control over third parties to which they want to share their personal information. In this case, the user should be made aware of what the third party can do with such access. (i.e. Can they download the personal information and use it in any way they desire, or only view the information online?)

1.4. Storage and transmission of personal information should be done in a reasonably secure manner.

1.4.1. Implementation Example: Transmission of personal information should be done with SSL or similar security.

2. Privacy Guidelines

Privacy should be a key part of the requirements and design of your software product. The requirements should be formed to ensure that the software product not only meets these privacy and security guidelines but complies with any regulatory requirements in the countries where you make the software product available. In addition, the code review process should verify privacy and security standards and policies.

Intel defines privacy as an individual's right to have a private life, to be left alone and to be able to decide when their personal information is collected, used or disclosed. Any information that can be used to identify, contact, or locate someone is considered personal information (e.g. name, address, telephone number, mobile phone number, e-mail address, social security number, government identification number, etc.). In addition, any information which is linked to personal information or from which other personal information can easily be derived is considered personal information too.

All developers have a role and responsibility in understanding privacy compliance requirements and associated risks[2]. Below is a summary that highlights what privacy compliance actions can be taken to mitigate certain business, consumer, and legal risks.

Compliance Requirements	Risks
• You should know what personal information their application's process, why, who has access to it and who you share it with (subsidiaries, vendors, etc.).	• Damage to your reputation, brand or business relationships
• You should handle personal information in line with Fair Information Practice Principles[3] (Notice, Choice, Access, Security, Purpose, Data Accuracy, Data Minimization, Data Retention, Data Transfer, and Redress)	• Legal liability and industry or regulatory sanctions
• You should protect personal information with reasonable security controls	• Charges of deceptive business practices
	• Customer distrust
	• Denial of consent by individuals to have their personal information used for business purposes
	• Disruption of international business operations
	• Termination of the application distribution agreement by Intel

Some data elements are considered more sensitive than others (e.g. biometrics, children's personal information, etc.) and may require additional compliance efforts with statutory rules and regulations. **You should review these with your legal counsel**.

3. Privacy Concepts in Application Development

When you develop an application that collects or uses, shares, stores, or transmits personal information, you will need to comply with international privacy rules and regulations The concepts described below can provide specific foundational requirement that should be comprehended within your application development efforts.

3.1. Purpose

Before any personal information collection, you should clearly define the reason

why you need to collect personal information prior to obtaining it from an individual. You may not use personal information for any other reason than the purpose specified to the individual at the time of collection without their prior consent, including secondary uses, like direct marketing purposes.

Recommendations on how to prepare for addressing the Purpose within your application

- Document your personal information business requirements.

- Document a data flow diagram

    - A list of the personal information that is collected, stored, shared, and transmitted
    - The method to protect the personal information
    - Methods of accessing the personal information
    - The user interface that can be used to control the data capture, storage, and transmission

- Document any considered secondary use of the personal information by the developer and third parties

  and subsequent notice requirements

3.2 Notice, Choice, and Consent

You should provide a clear explanation (Notice) of your personal information handling practices at the time of collection. The notice should be easy to find and easy to read. You should obtain affirmative opt-in consent[4] from an individual before collecting their personal information if required by law.

Recommendations on how to develop notice, choice, and consent into your application

- When installing an application or completing a registration form, configure the default to not collect personal information.
- Use radio buttons, check boxes, or menu selections to notify the individual of their choices and require the individual to select before proceeding.
- If an individual elects not to have personal information collected, allow the individual to participate as a guest if possible.
- Add a convenient location in your menu where individuals can revisit your personal information handling practices (e.g. privacy option in help menu, privacy footer in website).

- When transferring the personal information to third parties, you need to inform the individual. If an individual elects not to have personal information transferred to third parties, you need to honor their decision.
- Inform the individual for how long you will retain the personal information. Don't retain it for longer than required to meet your business objectives (e.g. not beyond the end of a support agreement) or to comply with applicable law.

- [4] Opt-in consent means that individuals must take some sort of affirmative action, indicating their desire to participate in a given program or service, like filling out a registration page, or submitting their email address to receive a newsletter.

3.3. Access to and Accuracy of Personal Information

You should provide individuals reasonable access to their personal information so the individual can ensure their personal information is accurate, complete and current.

Recommendations on how to develop access and accuracy into your application

- Create a secure user profile that requires a unique identifier and password combination to allow the individual to maintain their personal information.
- Organize all of the individual's personal information into a single menu selection or tab that displays all of their personal information for easy reviewing and editing.
- When an individual updates sensitive personal information, for example, passwords, or financial personal information, send a electronic message to the individual stating their <insert> personal information has been updated on <date time> by <e-mail address or unique identifier>

3.4. Minimization and Retention of Personal Information

You should collect and/or process only the personal information required for a specific purpose and not retain personal information longer than necessary to satisfy the purpose for which it was collected.

Recommendations on how to develop minimization and retention into your application

- If the individual's personal information is not needed, don't collect it. Deploy uses of pseudonyms[4] or unique identifiers where possible.
- Scrutinize the amount of required data elements. Look for opportunities to make personal information collections optional or not all.

- All personal information collected should have an expiration date associated with it. Formalize the lifecycle of data by developing a Data Retention Policy for all personal information data elements and include your practices in the privacy statement.

3.5. Security and Transfer of Personal Information

You should take reasonable measures to protect personal information from unauthorized access, use, modification, disclosure or loss. Recommendations on how to develop security into your application

- When collecting personal information on the wire, don't transmit in clear text. Implement encryption techniques like https or SSL.
- Allow the individual a menu of choice on how their information is disclosed. Allow selections from everyone to no one or allow the individual to generate their own customizations.

4. Security Controls to Preserve Privacy

To ensure individual's privacy is preserved and compliance to appropriate regulatory standards has been met certain security controls must be employed. The following are some of the vulnerabilities which lead to privacy violations:

- Injection flaws,
- Insecure Direct Object Reference,
- Information Leakage and Improper Error Handling,
- Broken Authentication and Session Management, and
- Failure to Restrict URL access.

Completing a code review and/or vulnerability scan will help to catch these vulnerabilities. You should develop security controls necessary to preserve the individual's personal information and account log-in information.

4.1. Input Validation

Input validation is the process of verifying the input, to ensure it is in the expected format. This involves checking for data length, type, syntax and correct business rules, before displaying or storing data. This mitigation against Cross-Site

Scripting (XSS) attacks is quite prevalent. Recommendations on how to perform input validation

- **There are multiple strategies for input validation, for instance whitelist and blacklist validation. It is** recommended, to do a combination of both. Utilize a whitelist to constrain input to the known good data and validate the format, length, and type. Then test for known malicious input using blacklist validation.
- Canonicalization is the process from converting data to its simplest form. Web applications utilize this process when converting form URL encoding to IP address. It is essential to be aware of potential canonicalization errors. Inputs must be decoded and then canonicalized before being validated. This is essential because an application should not decode the same input more than once because it could be used to bypass whitelist schemes.

4.2. Enforce Least Privileges

Individuals should only have the least amount of access or privileges to an application which allows them to complete their necessary objective. Following this recommendation can help to prevent individuals from having access to someone else's personal information or any other sensitive information. In addition, this concept can be used to limit access of a program or even a process. It is essential to determine the necessary information and resources to complete a legitimate task. Having a clear understanding of how data is flowing in the application will help to limit privileges. Recommendation on how to enforce least privileges

Always enforce the principal of least privileges for an individual's or process' access to any database or backend system. The access should be based on the privileges necessary to complete the business objective.

4.3. Information Leakage

Information leakage occurs when information about an application's configuration or internal workings are exposed. The information which is leaked could be sensitive data or could allow an illegitimate individual to gain access to the application. A common example is leaking information via an error message by showing debug information. Information leakage can also be more subtle such as revealing state information by the duration it takes to process certain operations.

Recommendations on how to prevent personal information disclosure

- All developers working on a single application should use a common approach to handle exceptions.
- Limit contents of error handling messages. An alternative to would be to create a default sanitized error message.
- Utilize similar or identical error messages.
- An additional mitigation strategy for sensitive transactions could be to implement random wait times for all transactions to hide this detail from an attacker.
- Different components in an application such as a database and web server will have different error messages. It is necessary to verify error messages and attempt to disable or limit detailed error handling.

4.4. Direct Object Reference

A direct object reference occurs when a developer displays a file, directory, database record, a key or any other type of reference. An attacker can use this information to get access without authorization. For instance, if an error message for an online store displays a database file location. An attacker could then download the database and gather information about the store's customers. This vulnerability can be detected using vulnerability scanning tools or a manual code review process. In addition, it could be avoided by using indirect methods such as an index or indirect reference map rather than putting the actual location of the file, directory, or etc.

Recommended controls to prevent direct object reference include

- Avoid displaying object references whenever possible.
- Object references should be validated using a whitelist or "accept known good" approach, i.e. verify paths for all directories.
- Confirm the user access the reference object has the necessary privileges and authorization.

4.5. Authentication and Session Management

HTTP cookies are often used to prove the individual has authenticated and to manage the session. Developers should avoid the usage of custom cookies. Flaws in authentication and session management usually involve failure to protect credentials and session tokens. This leads to session hijacking and the ability of illegitimate individuals to gain access to the application. This can be prevented my ensuring that login occurs on an encrypted page, and all credentials or session tokens are encrypted in transit using SSL. Methods for ensuing secure authentication and session management

- Use SSL to transmit all cookies which are used for authentication or session management, not just for the login page.
- Leverage session management frameworks with built-in session management instead of building your own.
- Upon successful authentication or a change in privilege a new session tokens should be generated.
- Pages should include a logout which will destroy cookies on the server and client-side.
- Application should include a timeout which is appropriate to the data classification.
- HTTP cookies should not contain any personal information.

5. Conclusion

Ensuring privacy of your customers and fellow developers is critical. Everyone has the right to be left alone and manage their personal information. As developers it is essential to not only know applicable rules and regulations, but to understand how privacy should be incorporated as part of the fundamental design of an application. Security can provide controls to support privacy but it is crucial to understand fundamental privacy philosophies.

Appendix: Privacy Compliance - Top 10 List

10. Children: You should not knowingly collect personal information from children under 13.

9. Transparency (Notice): You are required to provide transparency to individuals about what personal information we collect by >100 state, local and international laws.

8. Retention: You should not retain information longer than is necessary to achieve your business objectives or to comply with applicable law.

7. Choice: Opt-in gives the individual choice to consent to communication from you.You should consider implementing opt-in practices, although you may not always be required by law, to only contact individuals who have proactively expressed a desire to be contacted.

6. Spam: You may be subject to the CAN-SPAM Act in many situations and therefore should provide clear information in the email regarding the source of commercial emails, and details on how to unsubscribe.

5. Vendors: You must make certain your vendors comply with your privacy policies.

4. Sensitive Data: Many privacy laws classify certain categories of personal information as "sensitive" and greatly restrict their collection and processing. Sensitive data elements include ethnicity, race, political opinions, and sexual orientation. When dealing with these categories of data, you should contact your legal counsel.

3. International Transfer: The European Union substantially limits the international transfer of personal information. Intel has certified to a "safe harbor" to transfer such data to the US. (See: www.export.gov/safeharbor/ for more info on international transfer & safe harbor). If you don't

certify for safe harbor you should obtain explicit consent from individuals prior to transferring their personal information; review international transfers with your legal counsel.

2. Security Breach Notification: Over 40 US states have security breach notification requirements, and other countries are looking to pass similar laws.

1. Privacy Compliance: Intel may terminate your application distribution agreement if you violate applicable privacy legislation, or if end-users complain about your data processing activities.

---

[1] Federal Trade Commission overview of the Fair Information Practice Principles

[2] Defined by the AICPA

[3] Federal Trade Commission overview of the Fair Information Practice Principles.

[4] Pseudonymity has characteristics similar to anonymity in that you are not identifiable, but you can be tracked through an alias or persona that you have adopted.