Vetting Assistant Responses

# Q:

2.1 District personnel must ensure there is verifiable user consent for the collection, use and disclosure of personal information if there is no legal basis for using web apps/software/services as determined by law or established by regulators. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is stated that verifiable user consent is required for the collection, use, and disclosure of personal information if there is no legal basis for using web apps/software/services as determined by law or established by regulators.

# Q:

2.2 Unless consent is obtained, providers must allow users to maintain ownership of and be in control of the content they create and upload to the business web app/software/service. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is unclear whether the business web app/software/service explicitly requires consent for users to maintain ownership of and be in control of the content they create and upload. The agreement primarily focuses on the protection of intellectual property rights and the prevention of unauthorized distribution of usernames and passwords.

# Q:

2.3 Providers must offer consent options so that users can consent to the collection and use of personal information necessary to provide the service without consenting to the use or disclosure of that information to third parties for other purposes (e.g. marketing). is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, based on the provided context, providers must offer consent options to users. This allows users to consent to the collection and use of their personal information for the purpose of providing the service, without giving consent for the information to be used or disclosed to third parties for other purposes, such as marketing.

# Q:

is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the policies provided in the context, it appears that meets the criteria for compliance. The policies provided include an Online Privacy Policy, GDPR and Privacy Shield Compliance Policy, Terms of Use, End User License Agreement, Disclaimer, and Release of Liability, and Terms of Service. These policies cover important aspects such as data protection, privacy, and user rights.

# Q:

3. Collection is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the information provided, I don't have enough context to determine if the collection meets the criteria for compliance and policies. Can you please provide more details or specific policies related to the collection?

# Q:

3.1 Providers must collect only the personal information required to operate the business web app/software/service, e.g., no accessing browser history, contact lists, search terms, preferences, device identification, location, etc. unless directly related to providing the service. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, the web app/software/service should only collect personal information that is necessary for its operation. This means that the app should not access or collect browser history, contact lists, search terms, preferences, device identification, location, or any other personal information unless it is directly related to providing the service.

# Q:

3.2 When apps are to be downloaded onto mobile devices, providers must offer choices to users regarding disclosure of data on their device such as location, identifiers, contacts, etc. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the information provided, it is not explicitly stated whether the app provider offers choices to users regarding the disclosure of data on their device. Therefore, it is not possible to determine whether the app provider meets this criteria.

# Q:

3.3 Providers must never collect personal information covertly, i.e., without the user’s knowledge, particularly audio/video information via the user’s own device. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the vetting tool, the statement "3.3 Providers must never collect personal information covertly, i.e., without the user’s knowledge, particularly audio/video information via the user’s own device" emphasizes that providers should not collect personal information without the user's knowledge, especially audio/video information through the user's own device.   
  
To determine if a specific provider meets this criteria, we would need to review their policies and practices in context.

# Q:

3.4 User profiles and activity within the web app or service must be kept private so that they cannot be seen or collected by others unless the app/service itself is collaborative and requires this type of sharing. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the vetting results, it appears that the app/service meets the criteria of keeping user profiles and activity private, unless it is collaborative and requires sharing. The app/service takes measures to protect user profiles and activity by using cookies for identification, authentication, and security purposes. However, it is important to note that if the app/service is collaborative and requires sharing, user profiles and activity may be visible to others who have been granted access.

# Q:

3.5 Users should be allowed to create generic accounts for subordinate users (e.g. guests) and/or create profiles using as little personal information as possible, in order to avoid the excessive collection of personal information. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it does not explicitly state whether users are allowed to create generic accounts for subordinate users or create profiles using as little personal information as possible. It only mentions that account data and profile data may be processed for the purposes of operating the website or the app, providing services, and ensuring security. To determine if such options are available, it would be best to refer to the specific policies and procedures of SCRC or contact their support staff for clarification.

# Q:

is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the information provided, it appears that both SocioCultural Research Consultants, LLC (SCRC) and Dedoose have stated in their respective agreements that they will make every reasonable effort to comply with all applicable laws, ordinances, and regulations. SCRC specifically mentions compliance with municipal, county, state, and federal laws, while Dedoose mentions compliance with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework for users subject to GDPR. Both companies also emphasize the protection of copyright and trade secrets.  
  
However, it is important to review the specific compliance requirements and obligations outlined in the agreements and policies of SCRC and Dedoose to ensure full compliance.

# Q:

4. Use, Retention, Disclosure is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided policies, it appears that SCRC meets the criteria of Use, Retention, and Disclosure. They state that they may use and retain Personally Identifiable Information (PII) when you use their website, applications, or services. They also mention that they may share your information with other companies or individuals in certain circumstances, such as when they have your consent, need to provide the requested service, or to comply with legal processes. Additionally, they mention that you have the right to request corrections or modifications to your PII at any time. However, it is always recommended to review the complete privacy policy for a comprehensive understanding.

# Q:

4.1 Providers must use, disclose and retain personal information only for the purpose of providing the business web app/software/service. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is unclear whether the service meets the criteria of using, disclosing, and retaining personal information only for the purpose of providing the business web app/software/service. The context mainly focuses on the retention and deletion of personal data, as well as the disclosure of personal data to other parties for various purposes. It does not explicitly state that personal information is used solely for the purpose of providing the business web app/software/service.

# Q:

4.2 Providers must not benefit or profit from user personal information. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is unclear whether the statement "4.2 Providers must not benefit or profit from user personal information" is applicable. There is no specific information regarding whether providers can benefit or profit from user personal information in the given context. Further clarification or additional information is needed to determine compliance with this criteria.

# Q:

4.3 Providers must not profile users for marketing purposes or in ways that lead to unfair, unethical or discriminatory treatment. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is unclear whether or not the criteria mentioned in 4.3 is met. The policy does not explicitly state whether providers are allowed to profile users for marketing purposes or in ways that may lead to unfair, unethical, or discriminatory treatment. Further clarification or information is needed to determine compliance with this criteria.

# Q:

4.4 Providers must not repurpose user data or use it for research without express consent, unless authorized by statute or anonymized. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, there is no specific information regarding whether the entity meets the criteria of not repurposing user data or using it for research without express consent, unless authorized by statute or anonymized. Therefore, it is not possible to provide a definitive answer to your question.

# Q:

4.5 Providers must securely destroy or make anonymous in a timely manner all personal information that is no longer required to provide the app/software/service and they must explicitly identify retention timelines. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, the app or service does have a data retention policy. Personal information will be securely destroyed or made anonymous in a timely manner when it is no longer required to provide the app/software/service. The app or service explicitly identifies retention timelines, stating that personal data will be retained for a minimum period of 6 months following the user's termination of services and a maximum period of 24 months following the user's termination of services. However, in some cases, the retention period may be determined based on the same 6-month principle. It is important to note that the app or service may retain personal data for longer if it is necessary for compliance with a legal obligation or to protect the vital interests of individuals.

# Q:

is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it appears that the entity being vetted, SocioCultural Research Consultants, LLC (SCRC), meets the criteria for compliance and policies. SCRC states that they comply with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework, and they have certified their adherence to the Privacy Shield Principles with the U.S. Department of Commerce. They also commit to resolving complaints about the collection and use of personal information in compliance with GDPR and Privacy Shield Principles.  
  
Additionally, the context mentions that SCRC and Dedoose, LLC have copyright protection for their software and materials, and both companies are committed to complying with applicable laws and regulations.  
  
If you have any specific questions or concerns about compliance and policies, please provide more details so that I can assist you further.

# Q:

5. Security Safeguards is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, Security Safeguards meet the criteria for compliance. The policies provided by Security Safeguards include:  
  
1. Encrypted SSL tunnel: Security Safeguards establishes an encrypted SSL tunnel for communication between the client and server, using SSL TLS 1.3.  
2. Hashed login credentials: User login usernames and passwords are encrypted using a one-way hash algorithm (SHA-256 + per user unique salt) and transmitted securely across the SSL tunnel.  
3. Access control: Security Safeguards allows account owners and project administrators to set security and access privileges on a per-project basis through the Security Center.  
4. Compliance with industry standards: Security Safeguards follows various industry standards for data security, including SAS 70 Type II, ISO27001, NIST800-53, HIPAA, and PCI-DSS.  
5. Encrypted backups: Daily backups of project data are encrypted using SSL AES-256 and transferred to both Amazon S3 Storage system and Microsoft Azure blob storage for redundancy.  
6. Secure server login: Server login is accessible only through a private VPN connection with its own SSL tunnel and separate authentication. It is also protected by Windows secure login authentication using an AES encryption algorithm.  
7. Data breach response plan: Security Safeguards has a systematic plan for response and notification in the event of a data breach.  
  
While Security Safeguards strives to provide industry-standard security, they cannot guarantee complete data security and integrity. It is recommended that users adhere to the security protocols described and take diligence in protecting their data.

# Q:

5.1 The provider must have a comprehensive security program in place that is reasonably designed to protect the security, privacy, confidentiality, and integrity of user personal information against risks, (e.g., unauthorized access or use, unintended or inappropriate disclosure) through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, the provider must have a comprehensive security program in place that is reasonably designed to protect the security, privacy, confidentiality, and integrity of user personal information against risks such as unauthorized access or use and unintended or inappropriate disclosure. This program should include administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

# Q:

5.2 Providers must define the safeguards in place. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it does not explicitly mention the specific safeguards in place or the policies of a particular provider being vetted for compliance. Therefore, it is not possible to provide an answer to your question based on the given information.

# Q:

5.3 Providers must ensure that all vendors they use to provide the service implement the same security safeguards. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, I'm unable to determine if the vendor meets the criteria of ensuring that all vendors they use to provide the service implement the same security safeguards.

# Q:

5.4 Providers must ensure that all successor entities are obligated to implement the same security safeguards for personal information previously collected. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

I'm sorry, but I don't have enough information to determine if the entity meets the criteria of ensuring that all successor entities are obligated to implement the same security safeguards for personal information previously collected.

# Q:

5.5 Providers must have breach protocols in place. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided information, it is not possible to determine if the entity meets the criteria of having breach protocols in place. There is no specific information regarding breach protocols for providers.

# Q:

is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the policies provided in the context, it appears that meets the criteria for compliance. The policies include an Online Privacy Policy, GDPR and Privacy Shield Compliance Policy, Terms of Use, End User License Agreement, Disclaimer, and Release of Liability, Restricted Use of this Product and Disclaimer, Corrections or Modifications to PII, Confidentiality, Compliance with Law, and Copyright Notice; Reservation of Rights. These policies cover important aspects such as data protection, privacy, compliance with laws, and intellectual property rights. It is recommended to refer to the original documents for full details and to understand the rights and responsibilities outlined in these policies.

# Q:

6. Openness and Transparency is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is not possible to determine whether the criteria of "Openness and Transparency" are met. The information does not directly address this topic.

# Q:

6.1 Providers must communicate privacy notices, permissions, privacy policies, Terms of Service, contracts etc., in clear, specific and unambiguous language that explains to users how their personal information is being used, processed, disclosed and retained by the provider and any third parties. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, the document meets the criteria of communicating privacy notices, permissions, privacy policies, Terms of Service, contracts, etc. in clear, specific, and unambiguous language. This ensures that users understand how their personal information is being used, processed, disclosed, and retained by the provider and any third parties.

# Q:

6.2 Providers must make links to permissions, privacy policies and Terms of Service, etc., easy to find after the account has been created. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is unclear if the document explicitly states whether or not the criteria of making links to permissions, privacy policies, and Terms of Service easy to find after the account has been created is met.

# Q:

6.3 Providers must identify the third parties to which they disclose personal information for processing, the specific data elements involved, and a summary of protections/assurances in place. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, meets the criteria stated in 6.3. They must identify the third parties to which they disclose personal information for processing, specify the data elements involved, and provide a summary of the protections and assurances in place.

# Q:

6.4 Where providers use data for statistical analysis and profiling, for making subjective assessments, for predicting behaviour or as part of a decision-making process it should be clearly communicated by providers to users along with a mechanism to challenge these assessments. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the vetting tool, it is unclear whether the provider meets the criteria of clearly communicating the use of data for statistical analysis and profiling, as well as providing a mechanism for users to challenge these assessments. Further information or clarification is needed to determine compliance with this criteria.

# Q:

6.5 Providers must state whether or not the business app/service allows users to make personal information publicly available online. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it is not explicitly stated whether or not the business app/service allows users to make personal information publicly available online.

# Q:

6.6 Providers must directly inform users before changes are made to policies and terms of use, etc., before data is used in a manner inconsistent with the terms they were initially provided. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, providers must inform users before making changes to policies and terms of use that would result in the data being used in a manner inconsistent with the initial terms provided.

# Q:

6.7 Providers must disclose the presence and use of third party cookies and provide options for managing them. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it does not explicitly mention whether the criteria of disclosing the presence and use of third-party cookies and providing options for managing them is met. Therefore, I don't have enough information to answer your question.

# Q:

6.8 Provider must confirm that they are in compliance with all laws. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, it can be inferred that does meet the criteria of confirming that they are in compliance with all laws. The agreements mentioned in the context state that each party must exert every reasonable effort to comply with all applicable laws, ordinances, and regulations. Therefore, the provider must confirm their compliance with all laws.

# Q:

is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, meets the criteria for compliance and its policies provided in context.

# Q:

7. Access and Correction is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, "Access and Correction" meets the criteria for compliance. The policy states that users have the right to access and correct their personal data. They can access their personal data through their Account Workspace when logged into the app. If any inaccuracies or incompleteness are found, users have the right to have it rectified or completed.

# Q:

7.1 Providers must make available contact information of an operator who will respond to inquiries and challenges from users about privacy policies, data handling practices, accuracy, completeness and use of personal information. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

I'm sorry, but I don't have the information to determine whether the entity in question meets the criteria of making available contact information of an operator to respond to inquiries and challenges from users about privacy policies, data handling practices, accuracy, completeness, and use of personal information.

# Q:

7.2 Providers must have a mechanism for users to access, correct, erase, and download content they created in a useable format. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, both Dedoose and SCRC meet the criteria of having a mechanism for users to access, correct, erase, and download content they created in a usable format. Dedoose allows authorized users to delete project data through its user interface, while SCRC retains project data for a certain period after termination of services and allows users to regain access to their data upon specific written request. SCRC also provides the option for users to export all of their data at any time and will delete project data and user/account data upon authorized request.

# Q:

7.3 Users have the right to erasure of their data, including metadata inferences, assessments and profiles (if not required for administrative purposes by the provider or the school board) and providers will not charge a fee for this service. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Yes, according to the provided information, meets the criteria of allowing users to have the right to erasure of their data, including metadata inferences, assessments, and profiles. Providers are not allowed to charge a fee for this service, unless the data is required for administrative purposes by the provider or the school board.

# Q:

7.4 Providers must ensure that when a user deletes their work in their account created by an adminstrator where the administrator maintains exclusive administrative rights, the copies in the administrator account must disappear, also. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided information, it is not possible to determine whether the copies in the administrator account will disappear when a user deletes their work in their account created by an administrator.

# Q:

7.5 Providers must ensure that users have the ability to delete their own accounts. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, there is no specific information that directly addresses whether users have the ability to delete their own accounts. Therefore, further investigation or clarification is needed to determine if the criteria is met.

# Q:

7.6 Providers must not require users to surrender their copyright to their own work if they post it to the application or service’s site. is being vetted for compliance and its policies provided in context. Does meet this criteria?

# A:

Based on the provided context, I don't have enough information to determine if the criteria is met.