Portability Trust Model

The purpose of this Portability Trust Model is to 1) support coordination of data transfer relationships between two parties (i.e., Sender and Receiver, also referred to as "Transfer Party"), 2) articulate criteria about a Transfer Party's trustworthiness, and 3) facilitate understanding between Transfer Parties regarding their respective data processing practices.

DTI welcomes your feedback on version 2 of the model. For more on DTI's trust work, including relevant work on threat modeling and definitions, see our website trust landing page. You can help us to continue to mature the model by sharing your feedback online here.

Trust Criteria 1: Transfer Party Authentication.

Criteria: Authenticity of Transfer Parties is identified and can be communicated.

Questions:

- *Known Entity* - Is the Transfer Party a known and established entity?
    - Note: Transfer parties may incorporate existing entity authentication practices (e.g., validating legal entity identifiers)
- *Previous Entities* - Has the Transfer Party been known by other corporate names or a part of other entities?
- *Establishment* - How long has the Transfer Party been in operation?
- *Authenticator* - How can other Transfer Parties technically verify that they are interacting with the expected Transfer Party?
- *Agent* - How can a Transfer Party verify an agent acting on behalf of another Transfer Party?

Example Artifacts: Transfer Party authentication policies, processes, and procedures. Corporate documents, including information about incorporation and affiliated companies.

Relevant Risks Addressed: Spoofing, Denial of Service, Elevation of Privilege, Unauthorized Disclosure

Trust Criteria 2: Jurisdiction

Criteria: The geographic location(s), including data storage location(s) and relevant data protection or other common laws of a Transfer Party, are identified and communicated.

Questions:

- *Location* - What country or jurisdictions govern this Transfer Party's data practices or compliance?
    - Note: The jurisdiction, and compliance with applicable laws, may provide answers for additional Trust Criteria.
- *Compliance* - Does the Transfer Party have compliance obligations in other jurisdictions? What relevant compliance obligations would the Transfer Party like to share?
    - Note: This question allows Transfer Parties to proactively share compliance with laws such as data security, data protection, and government access.
- *Processors* - Does the Transfer Party pass down compliance obligations or other responsibilities to Processors, including the Receiving Party?

Example Artifacts: Transfer Party policies relevant to Transfer Data, such as jurisdiction-specific privacy policies, onward transfer policies, government access policies, etc. Information about Transfer Party incorporation and legal compliance. Attestations regarding processor responsibilities. If applicable, the Transfer Party's article 27 GDPR representative.

Relevant Risks: Non-Compliance

Trust Criteria 3: Data Security

Criteria: Data security practices are identified and communicated.

Sub-Criteria 3.1: Transfer Party Security Practices

Criteria: Transfer Party security practices are identified and communicated.

Questions:

- *Data security* - How is Transfer Party data secured against unauthorized access? What controls are in place?
    - Note: This includes access by unauthorized employees, partners, or outside actors.
- *Cybersecurity program* - Does the Transfer Party have a cybersecurity program in place?
- *Cybersecurity standards* - Does the Transfer Party adhere to specific cybersecurity standards? If so, please identify the applicable standard(s).
    - Note: Existing evidence of compliance with standards such as ISO 27001, ISO 27701, SOC2, and/or NIST standards should be leveraged to the greatest extent practicable to accelerate or simplify trust processes.

Example artifacts: Cybersecurity program documentation, relevant certification documentation (ISO certs, SOC2, 3rd-Party audit or assessment reports). Internal processes, policies, and procedures regarding authorized access.

Relevant risks: Tampering, Unauthorized Disclosure, Denial of Service, Elevation of Privilege, Repudiation, Non-Compliance

Sub-Criteria 3.2: Data Transfer Security Practices

Criteria: Transfer security practices are identified and communicated.

Questions:

- *Transfer security* - If accepting requests, does the Transfer Party reject requests that are over unsecured connections, and if sending requests, does the participant send using secured connections? If so, how is it secured?
- *Data authentication* - Can Transfer Data be authenticated by the Receiver?

Example Artifact(s:) Documentation of security controls related to security in transit, tamper resistance, and upon receipt of transfer. Note: this documentation may be covered by relevant certifications or audit reports.

Relevant Risks: Tampering, Unauthorized Disclosure, Denial of Service, Elevation of Privilege, Repudiation

Sub-Criteria 3.3 Safeguards Against Harmful Content

Criteria: Safeguards against harmful content are identified and communicated by the Sender; these questions are not designed to be asked of the Receiver.

- *CSAM program* - Does the Transfer Party have a CSAM Program in place?
- *Content security* - Is the data secured and free from malware or other malicious content, to the best of the provider's knowledge and determination?
- *Content moderation* - If appropriate, is user-provided or generated content moderated, screened, or otherwise checked by the originating Party? / Is any user-generated content monitored for CSAM, harmful content, hate speech, etc?
- *Intellectual property* - Does the Transfer Party have a program in place to request and manage notice of infringing content on their platform?

Example Artifacts: CSAM Program documentation, Content Moderation policies/procedures, or Trust and Safety Program documentation.

Relevant Risks: Non-Compliance, Harmful Content, Spoofing

Trust Criteria 4 : Transparency

Sub Criteria 4.1: End User Transparency

Criteria: Transfer Parties provide End Users with reliable information about applicable data processing practices including how data will be used.

Questions:

- *Service Type* - What is the nature of the service of the Transfer Party? How is this presented to the End User?
- *Non-Service Processing* - Are there purposes for which data will be processed outside of providing the service to the End User? What are they?
- *Transfer Transparency* - What End User transparency mechanisms are in place, such as a transfer notice, to provide End Users with information about how their data are processed before, during, and/or after a transfer?
- *Onward Transfer* - What promises are made to the End User regarding any onward transfer of data, including transfers of de-identified or aggregated data? Where can documentation of these commitments (e.g., ToS) be found?
- *Commitments* - What additional commitments regarding the data to be transferred, if any, are made to the End User?

Example Artifacts: Examples of user notice describing the nature of the service, screenshots of Transfer Party UI/UX demonstrating transparency mechanisms (e.g., notice that "These photos will be added directly to your public feed"), Transfer Party documentation such as End-User Instructions that include details such as how to set processing permissions for transferred data, Screenshot of End User notice(s) from both the Sender and Receiver, Privacy Policy applicable to the transfer. Notably, a Privacy Policy may answer all of these questions and questions from other Trust Criteria.

Relevant Risks: Inadequate Transparency, Unanticipated User Processing Permissions

Sub Criteria 4.2 Transfer Party Transparency

Criteria: Transfer Parties provide each other and the public with reliable information about their data processing practices related to data transfers.

Questions:

- *Privacy policy* - Does the Transfer Party have a Privacy Policy in place? If so, where can it be found publicly?
- *Terms of service* - Does the Transfer Party have Terms of Service? If so, where can they be found publicly?
- *Commitments* - Does the Transfer Party make additional commitments regarding the data to be transferred beyond those found in its Privacy Policy? If so, where can they be found, if public?

Example Artifacts: Public-facing notice describing the nature of the service, Transfer Party Privacy Policy, Terms of Service, documentation of other privacy and data use commitments (e.g., public-facing web page, press release, or blog(s)).

Relevant Risks: Inadequate Transparency, Non-Compliance

Trust Criteria 5 : End User Authentication and Authorization

Sub Criteria 5.1: End User Authentication

Criteria: End Users requesting a data transfer are properly identified and authenticated.

Questions:

- *End User Authentication* - What authentication method for End Users is in place by Sender?
    - Note: Existing mechanisms to validate user requests for personal data may be repurposed.
- *End User Authentication frequency* - Is a fresh authentication process initiated as part of a transfer request or is evidence of recent authentication such as a local device cookie sufficient?
    - Note: The appropriate authentication method and whether authentication is re-acquired or verified at time of transfer will depend in practice on context and use cases and are not necessarily symmetrical between Sender and Receiver.
- *End User Identity* - Is the user anonymous, pseudonymous, or identified?
    - Note: Receiver may or may not want to know more about the End User's real-world identity, but it may be useful or necessary in some contexts.

Example Artifacts: Transfer Party authentication policies and procedures applicable to transfers. Note: Transfer Parties may rely on applicable industry certifications, if applicable to the transfer.

Sub Criteria 5.2: Transfer Parties have obtained consent from End Users for the Transfer.

Criteria: Transfer Parties have obtained consent from End Users for the Transfer.

Questions:

- *Consent Mechanism* - How is consent for the Transfer obtained from the End User?
    - Note: Existing mechanisms to assess the risk of fraudulent activity and mechanisms for seeking parental consent for minor users in downloads may be used.
- *Recordkeeping* - Are records of consent for the Transfer maintained?
- *Transfer scope* - Is the End User given specific controls to include or exclude portions of the data in/from the transfer?

Example Artifacts: Screenshots of consent presentation, process for record of consent capture (can be requested on a case-by-case basis)

Relevant Risks: Unauthorized Disclosure, Unauthorized Transfer