Transfer Impact Assessment – working template

Publisher: T-NEX · Template version: 10 September 2026 · Language: English

Use this template to document an assessment of a specific transfer. It contains no assessment of a country, supplier or project. Download the Markdown file, open it in a text editor and replace the fields in square brackets. Add rows or sections for further data flows, parties and findings. Where a question does not apply, record “not applicable” with a reason; keep unknown information visibly unresolved.

Assign evidence identifiers, such as S-01 for sources and E-01 for technical evidence. Linked or retained records need to show the state actually assessed. A tick or a general supplier promise does not replace the reasoning.

0. Document and responsibility

Item	Entry
Organisation / project / service	[complete]
TIA identifier and document version	[complete]
Date of fact gathering / law assessed as of	[complete]
Reason: introduction, change, scheduled review or incident	[complete]
Responsible data exporter, legal entity	[complete]
Assessment coordinator, role and contact	[complete]
Specialist or legal assessment, role and contact	[complete]
Technical implementation and evidence, role and contact	[complete]
Participating importer and person providing information	[complete]
Entity or function authorised to make the final decision	[complete]
Related processing records, contracts, DPIA and permission models	[identifier, version, location]
Next intended review / reason for the interval	[date and reasoning; event-driven review also applies]

Working status of this completed version: [to be determined: gathering facts / assessment underway / questions unresolved / decision documented]. This is not an approval status. Record the decision, scope and reasoning exclusively in section 7.

Scope and boundaries: [In a few sentences, describe the service and data flows being assessed. Identify excluded activities and explain the boundary.]

1. Record the processing and data flows

Complete the following questions for each distinct data flow. A product name or cloud region does not identify the legal entities involved. Include administration, remote support, tickets, logs, test copies, backups, collaboration services and further recipients.

Data flow [identifier]

Question	Description and evidence
What triggers the flow, and why is it needed?	[Purpose, business step and necessity]
Which source sends which data to which destination?	[Systems, legal entities and evidence identifiers]
Whose data is involved?	[Categories, such as customers or employees; do not insert unnecessary real personal data in the template]
Which categories and identifiers reach the recipient?	[Fields; address Article 9 special categories / Article 10 data separately where relevant]
What volume, frequency and period are involved?	[Volume, continuing/one-off, intended duration]
Where is the data stored, accessed and processed further?	[Country for storage and actual access; include support and backups]
What permissions does the recipient have?	[Read, change, export, administer, manage keys; evidence the actual configuration]
Which further recipients or sub-processors are involved?	[Legal entities, countries, purposes and links to further flow identifiers]
How long is data retained, and how is it returned and deleted?	[System-specific periods, implementation and evidence]
What legal basis supports the underlying processing?	[Article 6 and, where relevant, Articles 9/10; contract/instructions; reference to the existing assessment]
Which transparency, data-subject-rights and security requirements apply?	[References and unresolved points; a TIA does not replace these assessments]

Classification of the data used: [personal / pseudonymised / anonymised / synthetic; explain and identify evidence]. Pseudonymised data generally remains personal data. An assertion of anonymity requires a substantiated assessment of non-identifiability; removing names alone is not sufficient evidence.

Data-flow overview: [Connect the flow identifiers in their actual order. Show which decision is intended to cover which onward transfer.]

Unknown or conflicting information: [Question, responsible person, evidence requested, due date and consequence for the assessment].

2. Assess the parties, roles and Article 3 position

Legal entity / identifier	Role in this flow	Establishment and relevant branch	Actual access countries	Contract / permission evidence
[complete]	[Controller / joint controller / processor / sub-processor; explain]	[complete]	[complete]	[complete]

Assess the three cumulative transfer criteria in EDPB Guidelines 05/2021:

Criterion	Finding: yes / no / unresolved	Reasoning and evidence
The exporter is subject to the GDPR for this processing.	[complete]	[Article 3(1)/(2)/(3), relevant establishment or other connecting factor]
The exporter makes personal data available to another entity.	[complete]	[Separate legal entity, role and access actually provided]
The importer is outside the EEA or is an international organisation.	[complete]	[Entity/country; not just server region]

Reasoned conclusion on the existence of a transfer: [complete]. An employee of the same legal organisation on a business trip differs from a separate supplier or another group company. Even where Chapter V does not apply to the specific circumstances, processing risks and Article 32 GDPR still require assessment.

Is the importer directly subject to the GDPR under Article 3 for this particular processing? [yes / no / unresolved; specific reasoning, source and specialist assessment].

This is separate from whether a transfer exists. Direct GDPR application to the importer does not automatically remove a third-country transfer. At the same time, Article 1 of the 2021/914 transfer SCCs scopes them to importers whose relevant processing is not subject to the GDPR. A different position requires a separate assessment of the applicable instrument; signing 2021/914 alone does not resolve its scope.

3. Determine the transfer basis, modules and contractual annexes

Possible basis	Specific assessment	Finding, reasoning and evidence
Article 45 GDPR: adequacy decision	Which current decision? Does it cover the territory, sector, recipient and processing? Where recipient-specific conditions apply, what is the current status and coverage?	[complete]
Article 46 GDPR: appropriate safeguards	Which instrument and precise scope? Are the required contracts, authorisations and safeguards effective?	[complete]
Article 49 GDPR: derogation for specific situations	Which specific derogation and conditions are relied on? Assess its scope and limits; do not use it as a general replacement for an unsustainable routine transfer.	[complete]

Chosen basis for each flow: [Instrument, legal provision, version, parties, evidence and reasoning].

Is a TIA required for these circumstances, and what does it cover? [complete]. CNIL associates a TIA with assessment of Article 46 instruments. Where Article 45 or a valid Article 49 derogation applies, document that finding; its conditions and other GDPR duties remain to be assessed. Mark unnecessary subsequent sections with a reason.

Where the 2021/914 SCCs are used

Relationship	Module	Selection / relevant flow
Controller to controller	1	[complete]
Controller to processor	2	[complete]
Processor to processor / sub-processor	3	[complete]
Processor to controller	4	[complete]

Explain scope and selection: [Connect the role assessment, Article 3 position and actual contract]. Clause 14 has a particular condition for Module 4: the EU processor combines personal data received from the third-country controller with personal data collected by the processor in the EU. Record whether this applies to the flow concerned and which clauses actually govern it.

Review the contractual records:

- SCC version, agreed modules/options, signature and relationship with other contractual provisions: [reference and assessment].
- Annex I: parties, transfer description and competent supervisory authority: [version, completeness and consistency with sections 1/2].

- Annex II: specific technical and organisational measures: [version and mapping to evidence in section 5].
- Sub-processing under Clause 9: [specific or general authorisation, parties, notification route and opportunity to object]. Complete Annex III where specific authorisation is used; document the applicable list/change procedure for general authorisation.
- For Modules 2/3: coverage of Article 28(3)/(4) and suitable instructions: [reference and assessment]. The 2021/915 clauses concern processing on a controller's behalf, but are not themselves an instrument for third-country transfers.
- Onward transfers: [appropriate provision for each further recipient, flow identifier and evidence].

4. Assess relevant third-country law and practice

For each relevant country and importer, establish which laws and practices affect the particular processing. Address public-authority access and the effectiveness of the chosen instrument. A general country profile is insufficient.

Source register

Source ID	Publisher / title / legal provision	Version and legal status	URL / retained record	Access date and finding verified
[complete]	[Prefer official primary sources; identify other information as such]	[complete]	[complete]	[complete]

Finding [identifier] for country [complete] and flow [complete]

Question	Specific finding with source ID and reasoning
Which provision or practice applies to the importer, and why?	[Sector, activity, jurisdiction, type of service or other connecting factor]
Which data can be requested or directly accessed?	[Categories, scope, systems affected, plaintext/access credentials]
What conditions, limits and procedures apply?	[Clarity of rules, trigger, scope, necessity and proportionality; exact references]
What independent oversight and effective remedies are available?	[Competence, accessibility and practical limits for data subjects]
Are there secrecy, disclosure or key-access obligations?	[Effect on notification, challenge and safeguards]
What is known about actual practice?	[Current reliable sources; identify importer statements separately]
Which information is missing or conflicting?	[Unresolved legal issue, contrary source, resolution route and consequence]

Question	Specific finding with source ID and reasoning
Which obligation in the transfer instrument could be affected?	[Specific clause/safeguard and connection to the flow]

Importer information about previous practice: [Nature and number of relevant requests, period, services covered, handling and available records]. A statement that no request has been received cannot carry the assessment alone. Where practical experience is considered, address Clause 14 and footnote 12 of the SCCs and include objective supporting evidence.

Combined legal/specialist assessment: [Which conclusion follows from which facts? What remaining uncertainty affects the decision? What additional information or expertise is needed?]

5. Supplementary measures and actual protective effect

Connect every measure to a particular finding in section 4. Distinguish intended measures from measures that have been configured and verified. Do not treat organisational or contractual promises as a solution to a technical or legal access problem without assessing their effect.

Measure / ID	Finding and flow addressed	Specific configuration / owner	Implementation status / evidence	Assessed effect and remaining limit
[complete]	[complete]	[complete]	[Planned / configured / verified; date and evidence]	[Complete with reasoning]

Complete the key and plaintext assessment separately

- Where is data encrypted, decrypted and processed in plaintext? [Systems and processing steps].
- Who holds, administers or can obtain keys or decryption rights? [Entities, countries, administrators, emergency access and evidence].
- Can the importer or a further recipient read the data for its task? [Specific technical check].
- Which legal access powers from section 4 could reach the data or keys? [Finding ID and assessment].
- For pseudonymisation, who holds additional information and what re-identification remains possible using available means? [Design, test and assessment].
- For minimisation or anonymous/synthetic test data, which fields and side channels still contain personal data? [Include tickets, logs and screenshots].
- Which functional limits or workflow changes are necessary for the measure to work? [Specific restriction, owner and evidence].

Encryption in transit or at rest does not automatically protect against access to plaintext at the importer. EDPB Recommendations 01/2020 address, among other things, situations where an importer needs plaintext and problematic public-authority access rules apply. Assess the actual circumstances and justify effectiveness; do not equate “encrypted” with “adequately protected”.

Conclusion after measures: [Is the required protection ensured for the described scope by measures actually implemented? Give reasoning and evidence; if unresolved, identify what is missing before a decision can be made.]

6. Implementation, checks and unresolved issues

Item / ID	Required action and acceptance criterion	Owner / due date	Evidence / result	Consequence if unfinished
[complete]	[complete]	[complete]	[complete]	[Affected flow, access or decision]

Check at least the following, where relevant to the flow:

- [ ] Contractual annexes and technical permissions describe the same state. Evidence: [complete].
- [ ] Agreed access restrictions and key responsibilities have been tested in practice. Evidence: [complete].
- [ ] Onward recipients, authorisations and change notifications are incorporated into the workflow. Evidence: [complete].
- [ ] Public-authority requests reach the correct functions; applicable notification/review duties can be carried out. Evidence: [complete].
- [ ] Suspension, access removal, return and deletion can be performed for the affected flow. Evidence: [complete].

A checked box records a check actually performed and evidenced. Replace an inapplicable item with a reason; do not mark unresolved checks as passed.

7. Decision, escalation and stopping where necessary

The decision must refer to the same flow, contract and configuration versions as the assessment. Commercial benefit does not replace the required protection. A planned measure cannot provide the justification for a transfer already underway.

Decision field	Entry
Data flows and versions assessed	[complete]
Chosen basis and its verified scope	[complete]
Sources, measures and evidence supporting the conclusion	[Identifiers and specific conclusion]

Decision field	Entry
Reasoned result	[Complete; no positive assessment is preset]
Flows not covered / remaining restrictions	[complete]
Authorised decision-maker, name/role and date	[complete]
Participating specialist/legal and technical reviewers, actual contribution and date	[Complete; do not assert a review that did not take place]

Chosen action and reasoning: [Describe the applicable position: assessment of the Article 45/49 case completed; the specified Article 46 transfer can proceed with evidenced safeguards; do not start while prerequisites remain unresolved; suspend a continuing transfer; end the transfer or change the architecture]. No option is preselected.

Where unresolved or protection is not ensured:

- Affected flow and immediately available access restriction: [complete].
- Person responsible for implementation and timing: [complete].
- Contract/data-protection functions to inform and applicable notification duties: [complete].
- Evidence required before resumption and authorised decision-maker: [complete].
- If ending: return/deletion, copies, evidence and further duties under the applicable instrument: [complete].

For the 2021/914 SCCs, address particularly Clauses 14–16 as applicable to the selected module. If the required protection cannot be ensured, the affected transfer must not begin or must be suspended.

8. Monitoring and reassessment

Trigger	How will it be detected?	Owner / notification	Assessment required before change or continuation
New recipient or sub-processor	[complete]	[complete]	[complete]
New storage or access country	[complete]	[complete]	[complete]
Changed data category, use or volume	[complete]	[complete]	[complete]
Different key control, permissions or architecture	[complete]	[complete]	[complete]
Change to applicable law, case law, practice or transfer instrument	[complete]	[complete]	[complete]

Trigger	How will it be detected?	Owner / notification	Assessment required before change or continuation
Public-authority request, security incident or indication of inability to comply	[complete]	[complete]	[complete]
Scheduled review date reached	[complete]	[complete]	[complete]

Change record:

Date / version	Trigger and changed facts	Sources/measures reassessed	Result / decision / next review
[complete]	[complete]	[complete]	[complete]

9. Sources and further working materials

This template is an original T-NEX working structure. The following primary sources were checked on 10 September 2026 for this template version. Record the current versions and country-specific sources additionally for the particular case.

- GDPR – particularly Articles 3, 6, 9, 28, 32, 35 and 44–49.
- SCCs 2021/914 – Article 1, modules, Clauses 14–16 and annexes.
- 2021/915 controller–processor clauses – particularly Clause 1(f).
- European Commission: current adequacy decisions.
- European Commission: SCC overview and scope.
- EDPB Guidelines 05/2021, version 2.0 – Article 3 and the transfer concept.
- EDPB Recommendations 01/2020, version 2.0 – supplementary measures.
- CNIL: final TIA guide and external ODS template, published 9 July 2025.
- CNIL Practical Guide, final version January 2025.