

Tool 2 — Neurodata Transfer and Access Decision Tool (Neuro-TADT)

Supplementary Table 7

Assesses whether the safeguards associated with the assigned tier can be implemented and maintained across a proposed sharing, repository, remote-access, cloud, federated or cross-border pathway, including the gated public-release branch (Step 3), the compatibility-class lookup (Step 6A), origin- and destination-side restrictions (Step 6B) and exporter/importer checks (Step 7). Produces four outcomes. Completion does not determine that a transfer is lawful.

Step	Question	Answer	Required action
<i>General instructions before using this tool: Assess the proposed transfer or access arrangement using the tier and safeguards identified in Supplementary Table 6. Wherever this Tool says "record", enter the information against the relevant step in the transfer and access section of the Neurodata Governance Assessment Record. Where the MDTAA applies, incorporate or reference that assessment in Schedule C and link it to the classification recorded in Schedule B. Record supporting evidence, outstanding actions and responsible persons. Continuing through the assessment does not authorise transfer or access. A later answer does not remove an earlier restriction or unresolved requirement. Before Step 7, complete the pathway lookup at Step 6A and the restrictions check at Step 6B; the actions recorded there are prerequisites for Outcome 1 or 2.</i>			
1	What are you planning to do with the neurodata? Example: Using an EEG dataset to train a machine learning model for early detection of Alzheimer's disease.	Internal use only with no external or cross border sharing or access to data.	Record the internal use and why no listed external or cross-border pathway applies. Apply the safeguards identified in Supplementary Table 6 and assess applicable statutory access and authorisation requirements. Record "Neuro-TADT not required for this arrangement" and end this Tool. Other applicable governance assessments remain required
1	What are you planning to do with the neurodata? Example: Using an EEG dataset to train a machine learning model for early detection of Alzheimer's disease.	Share with another institution; international transfer; repository deposit; cloud-hosted access; or AI platform or vendor access.	Record every selected pathway and the proposed activity. Continue to Step 2.
1	What are you planning to do with the neurodata? Example: Using an EEG dataset to train a machine learning model for early detection of Alzheimer's disease.	Unsure	Obtain clarification of the proposed storage, sharing, access and processing arrangements. Pause the assessment and do not begin the proposed transfer or external access. Return to Step 1 when the pathway is established.
2	Has the neurodata already been assigned a risk tier using (Tool 1) Supplementary Table 6? Example: The neurodata has been classified as Tier 2 (Moderate Risk) using the criteria in Supplementary Table 26 before planning further processing or sharing.	Yes	Record the tier, whether it is provisional or confirmed, the applicable safeguards and the (Tool 1) Supplementary Table 6 assessment reference. Carry forward all unresolved conditions and restrictions. A provisional tier may support pathway assessment but does not remove required review. Continue to Step 3.
2	Has the neurodata already been assigned a risk tier using (Tool 1) Supplementary Table 6? Example: The neurodata has been classified as Tier 2 (Moderate Risk) using the criteria in Supplementary Table 26 before planning further processing or sharing.	No	Complete (Tool 1) Supplementary Table 6 to get a risk tier assigned to the particular data object and proposed activity. Return to Step 2 after a tier has been assigned. If (Tool 1) Supplementary Table 6 cannot establish a tier and requires specialist review, select Final Decision Outcome 4 below.
2	Has the neurodata already been assigned a risk tier using (Tool 1) Supplementary Table 6? Example: The neurodata has been classified as Tier 2 (Moderate Risk) using the criteria in Supplementary Table 26 before planning further processing or sharing.	Unsure	Locate the existing classification and check that it covers the object, version and proposed activity. Complete or update records according to Supplementary Table 6 if the classification is absent or no longer applicable. Return to Step 2 when the tier and safeguards are established.

Step	Question	Answer	Required action
3	Who will receive or access the neurodata? Example: An approved research collaborator, an international research consortium, or a trusted cloud service provider processing the neurodata under a data processing agreement.	Named collaborating institution; repository; cloud provider; commercial partner; or AI developer. Select all that apply.	Record each recipient's name, role and proposed access or processing activity. Continue to Step 4.
3	Who will receive or access the neurodata? Example: An approved research collaborator, an international research consortium, or a trusted cloud service provider processing the neurodata under a data processing agreement.	Unknown recipients	Record which recipients remain unidentified. Obtain recipient information from the proposed collaborator, repository, provider or other responsible party. Do not begin transfer or access. Return to Step 3 once recipients are identified. If they cannot be identified, select Final Decision Outcome 4 below.
3	Who will receive or access the neurodata? Example: An approved research collaborator, an international research consortium, or a trusted cloud service provider processing the neurodata under a data processing agreement.	Public or unrestricted release (open repository deposit, open licence, public model weights, publication of participant-level supplementary data)	Record the release channel, licence and any registration or click-through conditions. Public release is permitted through this Tool only where (a) Tool 1 (Supplementary Table 6) records a confirmed Tier 1 or Tier 1b finding made for the public as recipient, or (b) for a model or other computational artefact, Tool 3 (Supplementary Table 8) Step 7 records leakage testing with no material exposure for the intended release conditions and a documented anonymity assessment. If neither condition is met, record 'Public release not supported by current classification' and either select Final Decision Outcome 3 (redesign: controlled access, gated or registered access, or federated access) or return the object to Tool 1/Tool 3 for further de-identification or testing. If a condition is met, record 'Recipients: public' at Steps 4 and 12, treat Step 5 as 'Downloadable copy', and continue to Step 6.
4	Can every recipient and subprocessor be identified? Example: All recipients are known by name, including collaborating institutions, cloud service providers, and any contracted subprocessors.	Yes	Record each recipient and subprocessor, its role and the information available about its access. Continue to Step 5.
4	Can every recipient and subprocessor be identified? Example: All recipients are known by name, including collaborating institutions, cloud service providers, and any contracted subprocessors.	No or Unsure	Request a complete recipient and subprocessor list from the responsible organisation or provider. Do not begin transfer or access while required identities remain unresolved. Return to Step 4 when the list is complete. If the required information cannot be established, select Final Decision Outcome 4 below.
4	Can every recipient and subprocessor be identified? Example: All recipients are known by name, including collaborating institutions, cloud service providers, and any contracted subprocessors.	Not applicable — public release recorded at Step 3	Record 'Not applicable: public release permitted under Step 3'. Continue to Step 5.
5	How will recipients access the neurodata or governed artefact? Example: The recipient can download and retain a local copy of the neurodata rather than accessing it only through a secure remote environment.	Downloadable copy	Record what may be downloaded, by whom and to which environment. Specify tier-appropriate controls for local storage, copying, access, onward sharing, retention and deletion. Continue to Step 6.
5	How will recipients access the neurodata or governed artefact? Example: The recipient can download and retain a local copy of the neurodata rather than accessing it only through a secure remote environment.	Remote or controlled access without downloading the underlying object	Record the access environment, authorised users and restrictions on downloading or exporting data and outputs. Specify access controls, logging and output review appropriate to the tier. Continue to Step 6.

Step	Question	Answer	Required action
5	How will recipients access the neurodata or governed artefact? Example: The recipient can download and retain a local copy of the neurodata rather than accessing it only through a secure remote environment.	Query-only or federated access	Record where processing occurs and what queries, outputs, gradients or other information may leave each environment. Specify controls on queries, outputs, access and logging appropriate to the tier. Continue to Step 6.
		Unsure	Obtain confirmation of the access modes and export capabilities from the recipient or infrastructure provider. Pause the assessment and do not begin access. Return to Step 5 when the access arrangements are established.
6	Will the neurodata be transferred to, stored in, or remotely accessed from another legal jurisdiction? Example: neurodata remains on a server in South Africa but is accessed remotely by researchers in Germany.	Yes	Record every relevant originating, receiving, hosting and remotely accessing jurisdiction, including relevant subprocessor locations. Continue to Step 7.
6	Will the neurodata be transferred to, stored in, or remotely accessed from another legal jurisdiction? Example: neurodata remains on a server in South Africa but is accessed remotely by researchers in Germany.	No	Record the locations and the basis for concluding that no cross-jurisdictional transfer, storage or remote access is involved. Continue to Step 7.
6	Will the neurodata be transferred to, stored in, or remotely accessed from another legal jurisdiction? Example: neurodata remains on a server in South Africa but is accessed remotely by researchers in Germany.	Unsure	Obtain location and remote-access information from the recipients and infrastructure providers. Do not begin transfer or access while relevant jurisdictions remain unresolved. Return to Step 6 when the locations are established. If they cannot be established, select Final Decision Outcome 4 below.
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	A1 (unified legal space)	Record 'A1: no transfer mechanism required'. The lawful basis for processing in both environments and any sector-specific or institutional condition remain required at Step 7. Continue to Step 6B.
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	A2 (convergent; adequacy-type recognition)	Record the adequacy decision, regulation or recognition relied on, its date and any scope limits (for example sectoral or organisational limits, as for Canada (commercial organisations) or the United States (DPF-certified organisations only)). Verify that the recipient falls within the scope; if it does not, treat the pathway as Class B. Continue to Step 6B.

Step	Question	Answer	Required action
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	B (standard transfer instrument)	Record the instrument required by the origin regime (see the Step 6B regime table and the MDTAA Transfer-Instrument Modules). Mark the corresponding MDTAA module for activation at Tool 4 (Supplementary Table 9) Step 2. Continue to Step 6B.
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	C (operationally conditional)	As for Class B, and in addition: mark Tool 4 Step 3 (Supplementary Safeguards Module) as required; require a documented transfer-risk or impact assessment at Step 7(i); and record the supplementary institutional, repository or technical safeguards that make the pathway navigable. Continue to Step 6B.
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	D (restricted in practice)	Record that the pathway is restricted. Default to Final Decision Outcome 3: redesign toward remote access, federated or query-only access, aggregation to Tier 1, or an alternative destination. Proceed with a transfer of participant-level data only where counsel in the origin jurisdiction documents a lawful mechanism and the authorisations required at Step 6B. Continue to Step 6B.
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	E (insufficient legal certainty)	Record that legal certainty is insufficient. Default to Final Decision Outcome 4 unless counsel in the origin jurisdiction documents a lawful mechanism; where that is done, treat the pathway as Class D. Continue to Step 6B.

Step	Question	Answer	Required action
6A	Pathway class. What is the compatibility class of the origin→destination pathway (and of each origin→hosting and origin→remote-access pathway) in Supplementary Data 2 (or the current online version of the matrix)? Record the matrix version and date. Where the destination is the United States or Canada, use the North American governance-unit analysis (Supplementary Figure 1) and record the applicable federal, state or provincial regime instead of a class. Example: Nigeria → Germany is Class B; Germany → Brazil was Class C at the study cut-off and is adequacy-based (Class A2) since 26 January 2026.	Not in matrix / Unsure	Record the gap. Obtain an origin-jurisdiction legal assessment and treat the pathway as Class C pending that assessment. Continue to Step 6B.
6B	Origin-side and destination-side restrictions. Using the Step 6B regime table (and Supplementary Data 3 for jurisdictions not listed), does any of the following apply? (a) a statutory prohibition on transferring this category of data or this type of database (e.g., LGPD art. 13 §2); (b) a localisation, serving-copy or in-country processing duty (e.g., Kenya reg. 26; Rwanda art. 50); (c) a requirement of prior authorisation, notification, licence or registration by a regulator before transfer or storage abroad (e.g., POPIA s. 57(1)(d); NCSA authorisation); (d) sanctions, export-control or national-security screening of the destination or recipient (e.g., US DOJ Data Security Program, 28 CFR Part 202; OFAC) where any Party is a US person or the data concern US persons; (e) a research export permit, ethics-committee export clearance or data-transfer approval required by the origin jurisdiction (e.g., NACOSTI; NHREC); (f) a destination-side import condition (registration, local representative, sectoral hosting certification such as HDS in France).	Yes (select all that apply)	Record each applicable restriction, the responsible Party, the competent authority and the evidence required. Where (a) applies, select Final Decision Outcome 3 (redesign so that no transfer of the prohibited category occurs, for example analysis within the origin environment with export of results only) or Outcome 4. Where (b)–(f) apply, mark each as a prerequisite: Outcome 1 may not be selected until the authorisation, registration, serving copy, screening or permit is documented; Outcome 2 may be selected where the action is pending. Continue to Step 7(i).
6B	Origin-side and destination-side restrictions. Using the Step 6B regime table (and Supplementary Data 3 for jurisdictions not listed), does any of the following apply? (a) a statutory prohibition on transferring this category of data or this type of database (e.g., LGPD art. 13 §2); (b) a localisation, serving-copy or in-country processing duty (e.g., Kenya reg. 26; Rwanda art. 50); (c) a requirement of prior authorisation, notification, licence or registration by a regulator before transfer or storage abroad (e.g., POPIA s. 57(1)(d); NCSA authorisation); (d) sanctions, export-control or national-security screening of the destination or recipient (e.g., US DOJ Data Security Program, 28 CFR Part 202; OFAC) where any Party is a US person or the data concern US persons; (e) a research export permit, ethics-committee export clearance or data-transfer approval required by the origin jurisdiction (e.g., NACOSTI; NHREC); (f) a destination-side import condition (registration, local representative, sectoral hosting certification such as HDS in France).	No	Record the basis for concluding that none applies, with reference to the regime table or Supplementary Data 3. Continue to Step 7(i).

Step	Question	Answer	Required action
6B	Origin-side and destination-side restrictions. Using the Step 6B regime table (and Supplementary Data 3 for jurisdictions not listed), does any of the following apply? (a) a statutory prohibition on transferring this category of data or this type of database (e.g., LGPD art. 13 §2); (b) a localisation, serving-copy or in-country processing duty (e.g., Kenya reg. 26; Rwanda art. 50); (c) a requirement of prior authorisation, notification, licence or registration by a regulator before transfer or storage abroad (e.g., POPIA s. 57(1)(d); NCSA authorisation); (d) sanctions, export-control or national-security screening of the destination or recipient (e.g., US DOJ Data Security Program, 28 CFR Part 202; OFAC) where any Party is a US person or the data concern US persons; (e) a research export permit, ethics-committee export clearance or data-transfer approval required by the origin jurisdiction (e.g., NACOSTI; NHREC); (f) a destination-side import condition (registration, local representative, sectoral hosting certification such as HDS in France).	Unsure	Obtain origin-jurisdiction and destination-jurisdiction review. Do not begin transfer or access. Return to Step 6B when established; if it cannot be established, select Final Decision Outcome 4 below.
7(i)	Exporter side. Under the law of the originating jurisdiction, have the following been identified and documented: the lawful basis or justification for the disclosure; the transfer mechanism indicated at Step 6A (or the reason none is required); the transfer-risk, transfer-impact, privacy-impact or data-protection assessment required for that mechanism or by the origin regime; the authorisations identified at Step 6B; the exporter's authority to make the present transfer or release under any upstream conditions (consent scope, ethics approval, repository or funder terms, community agreements); and the ethics, institutional and repository approvals required? Consider consent or another lawful basis, statutory transfer provisions, adequacy-type mechanisms, contractual safeguards, DPIAs, PIAs or other jurisdiction-specific assessments, regulatory authorisation and institutional approval, as applicable.	Yes	Record each item with its reference and status. Verify the Data Exporter's authority to make the present transfer or release, including applicable upstream conditions. Mark outstanding items as pending. Continue to Step 7(ii).
7(i)	Exporter side. Under the law of the originating jurisdiction, have the following been identified and documented: the lawful basis or justification for the disclosure; the transfer mechanism indicated at Step 6A (or the reason none is required); the transfer-risk, transfer-impact, privacy-impact or data-protection assessment required for that mechanism or by the origin regime; the authorisations identified at Step 6B; the exporter's authority to make the present transfer or release under any upstream conditions (consent scope, ethics approval, repository or funder terms, community agreements); and the ethics, institutional and repository approvals required? Consider consent or another lawful basis, statutory transfer provisions, adequacy-type mechanisms, contractual safeguards, DPIAs, PIAs or other jurisdiction-specific assessments, regulatory authorisation and institutional approval, as applicable.	No or Unsure	Identify the missing basis, mechanism, assessment, approval or evidence of authority. Obtain the necessary origin-jurisdiction legal, ethics, institutional or repository review. Do not begin transfer or access. Return to Step 7(i) when documented. If no applicable lawful pathway can be established, select Final Decision Outcome 4 below.

Step	Question	Answer	Required action
7(ii)	Importer side. Under the law of each receiving, hosting and remotely accessing jurisdiction, have the following been identified and documented: the recipient's own lawful basis or justification for processing (including any special-category, health-data or sensitive-data condition); any registration, notification, licensing, local-representative or data-protection-officer requirement applying to the recipient; any sectoral hosting requirement (for example health-data hosting certification); and the recipient's ethics or institutional approval for the proposed use?	Yes	Record each item with its reference and status. Continue to Step 7A.
7(ii)	Importer side. Under the law of each receiving, hosting and remotely accessing jurisdiction, have the following been identified and documented: the recipient's own lawful basis or justification for processing (including any special-category, health-data or sensitive-data condition); any registration, notification, licensing, local-representative or data-protection-officer requirement applying to the recipient; any sectoral hosting requirement (for example health-data hosting certification); and the recipient's ethics or institutional approval for the proposed use?	No or Unsure	Identify the missing item and obtain destination-jurisdiction review. Do not begin transfer or access. Return to Step 7(ii) when documented; if it cannot be established, select Final Decision Outcome 4 below.
7A	Does the proposed activity require a statutory access authorisation, data permit or research permit under the origin regime or the hosting regime? Examples: a Findata permit (Finland); a Health Data Hub/CESREES authorisation (France); a Forschungsdatenzentrum authorisation (Germany); a Garante authorisation under art. 110 of the Privacy Code (Italy); a NACOSTI permit (Kenya); a UNCST clearance (Uganda); a COSTECH permit (Tanzania); CONEP approval of an international collaboration (Brazil); or, from 26 March 2029, an EHDS data permit.	Yes	Record the competent body, required authorisation, application or approval status, and reference. Record the authorised purpose, users, duration, processing location and release conditions once established. Mark an authorisation not yet obtained as pending; do not begin the activity requiring it. Continue to Step 8.
		No	Record the basis for concluding that no such authorisation is required for this activity. Continue to Step 8.
		Uncertain	Obtain review of the authorisation requirement. Do not begin the affected transfer or access. Return to Step 7A when the requirement is established. If it remains unresolved, select Final Decision Outcome 4 below.
8	Can the receiving or accessing governance environment implement and maintain the safeguards required for the assigned tier? Consider institutional oversight, repository governance, technical controls, contractual compliance, auditability, enforcement and available remedies.	Yes	Record the evidence of capacity to maintain the required safeguards. Identify any safeguards that the environment can support but has not yet implemented, for verification at Step 13. Continue to Step 9.
		No	Record which required safeguards cannot be maintained and why. If an alternative access model or governance arrangement could provide the required protection, select Final Decision Outcome 3 below. If no feasible alternative is identified, select Final Decision Outcome 4 below.

Step	Question	Answer	Required action
		Unsure	Record which safeguards cannot yet be verified. Request evidence from the recipient or provider (policies, certifications, repository governance documents, audit or penetration-test reports, Annexure 5 self-assessment). Do not begin transfer or access until capacity is verified. Return to Step 8 when evidence is available. If evidence cannot be obtained, select Final Decision Outcome 3 where an alternative access model could provide the required protection; otherwise select Final Decision Outcome 4 below.
9	Will the neurodata be linked with additional datasets after transfer or access? Examples include genomic, electronic health-record, wearable-device, consumer or public-register data.	Yes	Record the additional datasets, linkage purpose, responsible party and proposed resulting object. Apply Supplementary Table 6 to the proposed linked dataset or resulting object before linkage begins. Update the tier and safeguards recorded at Step 2 and review Steps 3–8 and 7A against that assessment, revising affected answers. Once the affected checks are complete and no blocking outcome applies, continue to Step 10. Do not repeat the same linkage assessment unless relevant circumstances change.
		No	Record that linkage is outside the assessed arrangement and requires reassessment before introduction. Continue to Step 10.
		Unsure	Record that linkage has not been excluded. Prohibit linkage contractually pending clarification (activate Tool 4 (Supplementary Table 9) Step 12 in its prohibitory form). Obtain confirmation from the recipient. Return to Step 9 when the answer is established; if it remains unresolved at the Final Decision, Outcome 1 may not be selected.
10	Will the neurodata or a derivative artefact be used to train, fine-tune, validate, benchmark or deploy an AI or machine-learning system? Example: An external collaborator will use a transferred EEG dataset to fine-tune a model for detecting cognitive impairment, or use the dataset to validate the performance of an existing predictive model.	Yes	Record the proposed AI activities, system, responsible parties and intended outputs. Complete Tool 3 (Supplementary Table 8) for the proposed activity and follow its Final Decision instructions. If the tier or safeguards change, update Step 2 and repeat the affected pathway checks before continuing. If Tool 3 (Supplementary Table 8) requires unresolved specialist review or prohibits proceeding in the current form, select Final Decision Outcome 4 below. Otherwise, continue to Step 11, carrying forward all outstanding safeguards and restrictions.
		No	Record that these AI activities are outside the assessed arrangement and require assessment before introduction. Continue to Step 11.
		Unsure	Obtain confirmation of the intended AI activities from the recipient. Prohibit unassessed AI use pending clarification. Return to Step 10 when the answer is established. If the intended use cannot be established, select Final Decision Outcome 4 below.

Step	Question	Answer	Required action
11	Will the neurodata be used for a purpose materially different from the approved research purpose? Examples may include commercial development, employment, insurance, clinical deployment or unrelated secondary research where these activities fall outside the already approved purpose, consent, ethics approval or other applicable authorisation. Interpretive note: Assess the proposed purpose against the authorisations and conditions applicable to this activity, including upstream restrictions and relevant consent, ethics and institutional requirements. A purpose different from the original study is not automatically prohibited, and public availability does not automatically authorise it. Record the basis for permitting the proposed use or the additional review or approval required.	Yes	Record the proposed purpose and the gap between it and the approved purpose, the consent, the ethics approval and any upstream condition. Do not begin the new use. Obtain the approvals required under Applicable Law and institutional rules: an ethics amendment; re-consent, or a documented compatibility or secondary-use assessment where the origin regime permits research reuse without re-consent; Data Access Committee approval; and the Data Exporter's written approval. If the proposed purpose is commercial or involves product development, licensing or deployment, mark Tool 4 (Supplementary Table 9) Step 10 as required and Step 11 as not applicable. If the proposed purpose is clinical deployment, record the applicable medical-device or clinical-governance requirements under Tool 4 Step 19. Return to Step 11 when approvals are documented; otherwise select Final Decision Outcome 4 below.
		No	Record the approved purpose and the authorisation or conditions covering it. Continue to Step 12.
		Unsure	Clarify the proposed purpose with the recipient and compare it with applicable authorisations and restrictions. Do not begin the uncertain use. Return to Step 11 when the answer is established. If it remains unresolved, select Final Decision Outcome 4 below.
12	May the recipient disclose, transfer, or provide access to the neurodata or resulting artefacts to another party? This includes collaborators, repositories, vendors, cloud providers, subprocessors and downstream recipients.	Yes	Record permitted onward recipients or recipient categories, purposes and conditions. Check that onward permission is consistent with upstream conditions. Distinguish permission already granted from permission requiring separate approval. Require applicable safeguards to continue throughout the onward pathway and mark outstanding approvals as pending. If the proposed onward arrangement introduces recipients, locations or access modes not yet assessed, update Steps 3–8 and 7A before continuing. Continue to Step 13.
		No	Record and contractually implement the prohibition on onward transfer or access. Continue to Step 13. This prohibition concerns the recipient's onward sharing; authority for the Data Exporter's present transfer remains subject to Step 7.
		Unsure	Clarify the onward-sharing permissions and upstream restrictions. Do not permit onward sharing while permission remains unresolved. Return to Step 12 when the answer is established. If the arrangement cannot be assessed without resolving this issue, select Final Decision Outcome 4 below.
12		Public release recorded at Step 3	Record that onward use is governed by the licence selected at Step 3 and that no further recipient-specific control is possible. Confirm that the licence prohibits re-identification and requires attribution and notification of suspected re-identification. Continue to Step 13.

Step	Question	Answer	Required action
13	Have all legal, institutional, repository, technical and contractual safeguards required for the assigned tier and proposed pathway been implemented and documented? Example: Before an international transfer of Tier 3 MRI data, the parties have confirmed the applicable transfer mechanism and approvals, implemented encrypted transfer and role-based access, enabled audit logging, restricted onward sharing, and documented permitted uses, retention, deletion and incident-response requirements.	Yes	Record the implementation evidence and responsible verifier. Proceed to the Final Decision below and check the conditions for Outcome 1. Outstanding requirements identified earlier must still be satisfied.
		No, but they can be implemented.	Record each outstanding safeguard, the responsible party and the evidence needed to verify implementation. Proceed to the Final Decision below and select Outcome 2 only if its conditions are met. Do not begin transfer or access before implementation is verified.
		No, and they cannot be implemented within the proposed pathway	Record the safeguards that cannot be implemented. Select Outcome 3 if a feasible alternative arrangement may provide the required protection. Otherwise, select Final Decision Outcome 4 below.
		Unsure	Obtain verification from the responsible technical, legal or governance reviewer. Do not begin transfer or access. Return to Step 13 when implementation can be established. If material uncertainty remains, select Final Decision Outcome 4 below.
<i>Final Decision: Select and document one outcome Interpretive note: A Neuro-TADT outcome provides structured governance decision support. It does not independently authorise processing, establish formal legal adequacy or replace any required legal, ethics, institutional, repository or regulatory determination.</i>			
	Outcome	Decision Criterion	

Step	Question	Answer	Required action
1	Proceed subject to applicable approvals	Select only where the applicable lawful basis, transfer or access mechanism, required approvals and authority for the present transfer have been confirmed, and all required safeguards are implemented and documented. Record the approved recipients, purposes, access conditions, supporting evidence and reviewer. Proceed only within those confirmed approvals and conditions. Reassess before a material change to the object, purpose, recipient, jurisdiction or access arrangement. Outcome 1 may not be selected while any Step 6B prerequisite, Step 7(i)/(ii) item or Step 9 uncertainty remains open. For public release, Outcome 1 additionally requires the Tier 1/1b or model-anonymity condition at Step 3 to be confirmed, the licence to be recorded, and a takedown and re-identification-response procedure to be documented.	

Step	Question	Answer	Required action
2	Proceed after supplementary safeguards are implemented	Select where the applicable legal and approval prerequisites are established, but specified safeguards remain to be implemented within the current pathway. Record each outstanding safeguard, responsible party and verification requirement. Withhold transfer or access until implementation is verified. Return to Step 13 and, if all conditions are satisfied, record Outcome 1.	
3	Redesign the transfer or access pathway	Select where required safeguards cannot be maintained under the current arrangement but a feasible alternative may provide the required protection. Record why the current pathway is unsuitable and the proposed changes. Do not begin transfer or access through the unsuitable pathway. Repeat this Tool for the redesigned arrangement, updating Supplementary Table 6 if the changes could affect functional exposure or the required tier.	

Step	Question	Answer	Required action
4	Do not proceed and obtain specialist review	Select where a required legal basis, mechanism, approval, recipient identity or material governance issue remains unresolved, or the required protection cannot be maintained. Record the reason, required review and responsible person or body. Do not begin the affected transfer or access. Following review, return to the affected step and update all dependent answers. If no acceptable pathway is established, retain this outcome.	

Neurodata Governance Toolkit, version 1.0 (October 2026). Governance decision support only; not legal advice.