

APPENDIX V

MODEL SWISS DATA SHARING AGREEMENT WITH DIGITAL SELF-DETERMINATION CLAUSES

APPENDIX V

Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses

This appendix reproduces an existing IPI Subscription Agreement for Access to Technical Data (Unilateral) and illustrates how considerations related to Digital Self-Determination can be reflected within an established contractual framework. The clauses in orange were added as part of this project to demonstrate how DSD-aligned governance elements such as transparency, purpose limitation, accountability, and review mechanisms can be embedded in data sharing agreements. Text shown in blue and red originates from the original IPI template and has not been substantively altered.

This model is provided as a reference example to support data space operators and legal teams in exploring how DSD considerations may be translated into contractual practice. While the example focuses on a subscription agreement for access to technical data, similar adaptations could be made to the other IPI template agreements for data exchange and data transfer.



IPI – Subscription Agreement (commented)

VERSION: OCTOBER 2023

SUBSCRIPTION AGREEMENT FOR ACCESS TO TECHNICAL DATA (UNILATERAL)

COVER SHEET

Date	[date]
Data Holder	[name / company name / address] Contact: [name] [email address]
Data Recipient	[name / company name / address] Contact: [name] [email address]
Designated Data Steward / Contact Point	Name, function, and email of the Data Holder's Data Steward. Name and email of the Data Recipient's operational contact.
Context Change Review	[Yes/No: Parties intend to use the Context Change Review mechanism. Frequency (if any): annually / upon notice only.]
Covered Data	[describe the Data to which Data Recipient shall have access under this agreement, including documentation relating to such Data, their format, etc.]
Access	[specify the platform on which the Data Recipient subscribes to obtain regular access to the Covered Data or the API made available to the Data Recipient to allow access to the Covered Data, or any other technical means by which access will be provided]



Subscription Term and Notice	[specify the duration of the initial term for which the Data Recipient subscribes, e.g. 1 month, 1 year, etc.] Termination Notice: [specify the duration of the advance notice that must be given to terminate the agreement, e.g. 1 week, 1 month, etc. – it must be shorter than the Term]
Subscription Fee	[select an option and insert the amount and recurrence of the Subscription Fee if access is granted against a fee] [Alt.1] CHF [insert price] [+ taxes] of [yearly] / [quarterly] / [monthly] Subscription Fee [Alt.2] Free
Use Restrictions	[specify the restrictions that will apply to the use of the Covered Data; multiple boxes may be checked] No Commercial Use of the Covered Data No Commercial Use of the Results No Distribution of the Covered Data No Distribution of the Results Research-only Internal use only

1. DEFINITIONS

The capitalized terms in this Agreement have the following meanings:

Commercial Use	any use of the Covered Data and/or of the Results by the Data Recipient or a Downward Recipient that is primarily intended towards a monetary compensation or commercial advantage.
Confidential Information	any proprietary and/or non-public information provided by either party, in particular but not limited to trade secrets or know-how or other related proprietary business information and data, whether such information is provided in tangible or intangible form, written, oral, graphic, pictorial or recorded form or stored on computer discs, hard drives, magnetic tape or digital or any other electronic medium.

Context Change	any material change in the intended use or purpose of the Covered Data, in the technical or societal environment in which the Covered Data is used, or in the risks, impacts, or expectations associated with such use, including new foreseeable effects on individuals, groups or communities represented in or affected by the Covered Data.
Covered Data	any Data made available under this Agreement as defined on the cover sheet, to the exclusion of any communication Data automatically generated by the parties for the purpose of allowing the Data Recipient to access the Covered Data.
Data	any digital representation of acts, facts or information and any compilation of such acts, facts or information, to the exclusion of Personal Data, of any type and in any format.
Data Steward	the individual or individuals designated by each Party as responsible for overseeing responsible data practices, reviews alignment with Digital Self-Determination principle, and serving as the primary point of contact for all notices, concerns, or matters relating to the responsible use, governance, review, or modification of the Covered Data.
Digital Self-Determination	the principle that individuals, groups or communities whose interests may be affected by the Covered Data retain agency, clarity and control over how such data is accessed, used, shared and interpreted. This includes transparency regarding the Covered Data and its use, contextual purpose limitation, the ability to review or request modification of certain uses if risks change, and where appropriate the involvement of relevant stakeholders in governance or review processes.
Distribute	make all or part of the Covered Data available to third parties in unmodified form or in such modified form that would still allow such third party to retrieve the original Covered Data.
Downward Recipient	any person or entity to whom the Covered Data is made available by the Data Recipient, directly or indirectly.
Harm or Misalignment	any use, effect, or outcome of the Covered Data or the Results that contradicts the legitimate expectations, interests, or rights of individuals, groups or communities represented in or affected by the Covered Data, including newly emerged risks not reasonably foreseeable at the time of the Agreement. It triggers the review/mitigation mechanisms in this Agreement and is not a stand-alone restriction outside the agreed process.
Intellectual Property Rights	all intellectual property rights, whether registered or not, and anchored in either national or international law, in and to the Covered Data, including without limitation copyright, trademark right, patent right and database right.

Interoperability	the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use Data in order to perform their functions.
Personal Data	any data or information relating to an identified or identifiable person within the meaning of article 3 let. a of the Swiss Data Protection Act (DPA – RS 235.1).
Restrictions	the restrictions on use specified on the cover sheet.
Results	any results obtained, developed, created or improved by the Data Recipient based on its use of the Covered Data.

2. GENERAL PROVISIONS

2.1 Access. Subject to the terms of this Agreement, the Data Holder grants the Data Recipient access to the Covered Data in accordance with the access modalities set forth on the cover sheet for the Term, in the format set forth on the cover sheet. Access to the Covered Data includes access to any updates of such Covered Data or newly collected Covered Data, if any. To support Digital Self-Determination, the Data Holder shall provide, in a clear and accessible manner, the information reasonably necessary for the Data Recipient to understand the structure, limitations, provenance and context of the Covered Data, including any known impacts the Covered Data may have on identifiable groups or communities.

[Drafting comment: “Reasonably necessary” becomes not subjective or vague: it refers only to the information specified in the Cover Sheet, the defined terms in Section 1, the elements expressly listed in this clause (structure, limitations, provenance, context and known impacts), and the Data Holder’s existing documentation and actual knowledge. It is therefore a limited, evidence-based standard and not an open-ended obligation.]

2.2 Subscription Fee. [Alt.1] Access to the Covered Data is provided against payment of the non-refundable Subscription Fee, payable in advance and at the frequency mentioned on the cover sheet. [Alt.2] No Subscription Fee shall be charged to provide access to the Covered Data and each party shall bear its own costs relating to implement and maintain the relevant tools allowing for such access.

[Comment: select Alt.1 if the access is granted against payment of a fee and Alt.2 if access is granted for free.]

[DSD addition (optional): Upon request, the Data Holder shall provide a short explanation of the elements composing the Subscription Fee to support transparency and informed decision-making.]

2.3 [Fee Calculation. The Subscription Fee shall not exceed the costs directly related to making the Covered Data available to the Data Recipient.]

[**Drafting comment:** section 2.3 reflects the principle applicable under art. 9 of the Data Act. This provision states that when the data recipient is a SME, the agreed compensation shall not exceed the costs directly related to making the data available and that are attributable to the data request of the data recipient.]

2.4 No-Exclusivity. The Covered Data is provided on a non-exclusive basis and the Data Recipient acknowledges that the Data Holder may grant access to the Covered Data to third parties or may continue to use the Covered Data itself.

2.5 Restrictions on Use. The use of the Covered Data by the Data Recipient and/or any Downward Recipient, if any, shall be limited by the Restrictions.

2.6 Prohibited Use. In addition to any Restrictions, the Data Recipient and the Downward Recipient, if any, shall not:

- a) deploy any coercive means or abuse any evident gaps in the technical infrastructure of the party holding the Covered Data, to obtain access to Data;
- b) use any Covered Data or Result to derive insights about the economic situation, assets and production methods of, or use by the Data Holder, that could undermine the commercial position of the Data Holder on the markets in which such party is active unless such party has consented to such use and has the technical possibility to withdraw that consent at any time;
- c) use any Covered Data or Result to develop a product or service that competes with the product or service from which the Covered Data originate or share such Data with a third party for that purpose.

[**Drafting comment:** this section addresses potential risks related to the use of Covered Data by the data recipient. It is based on obligations applicable under the Data Act to the data recipient or data holder, as the case may be (e. g. art. 5 and 6 of the Data Act). Since this agreement is bilateral, does not involve any individual and is not based on any legal requirement to share data or any access right, the obligations fall upon the data recipient only.]

DSD additions:

- d) use the Covered Data or Results to infer sensitive attributes, behavioral patterns or profiling information relating to identifiable groups or communities, unless explicitly authorized and supported by appropriate safeguards;
- e) use the Covered Data in a manner that creates foreseeable Harm or Misalignment, as defined in this Agreement;

- f) continue a specific use if the Data Holder notifies the Data Recipient that a Context Change has occurred and the Parties have not yet reached agreement on appropriate safeguards or whether the use may continue.

[Note: These refinements integrate DSD's harm mitigation, group-level protection, and dynamic governance.]

2.7 Limited License. This Agreement does not aim at addressing or governing possible ownership or property rights in or to the Covered Data. To the extent that the Covered Data shall however be subject to Intellectual Property Rights, the Data Holder hereby grants the Data Recipient a non-exclusive license to the Data Recipient to use the Covered Data in accordance with this Agreement, for the Term.

2.8 Confidentiality. The Covered Data may contain Confidential Information of the Data Holder or third parties and the Data Recipient agrees that this Agreement does not constitute permission to obtain or reveal Confidential Information, whether by way of reverse-engineering or decompiling, or any other technical or non-technical mean allowing access to such Confidential Information. The Data Recipient shall treat as confidential any Confidential Information it may receive or be granted access to unwillingly or fortuitously by the Data Holder. The Data Recipient shall also refrain from any use of Covered Data or Confidential Information that would reasonably be expected to undermine the trust, expectations or self-determination interests of individuals, groups or communities represented in the Covered Data.

2.9 Compliance. Nothing in this Agreement shall restrict, limit or otherwise affect any rights or obligations that the Parties may have under any applicable laws or regulations, such as (without limitation) competition and antitrust laws, or in relation to data sharing or data access requests of users.

[Drafting comment: this section reserves any obligations a party may have under the Data Act or other laws or regulations, since the Data Act imposes specific data sharing obligations on data holders. Even if the Data Act is not directly applicable to the relationship between the parties under this agreement, it may nevertheless apply to a party depending on the circumstances (e.g. if such party provides connected products or services in the EU).]

DSD addition: For the avoidance of doubt, the Parties acknowledge that this Agreement is intended to operate consistently with principles of Digital Self-Determination as defined herein and shall cooperate in good faith to address any new regulatory requirements or sector-specific standards that reinforce such principles.

2.10 [Audit. The Data Recipient agrees that the Data Holder may, at any time during the Term, but no more than once a year, access the Data Recipient's books, records, infrastruc-

tures, databases and Results in order to ensure compliance with the present Agreement. Any Confidential Information of the Data Recipient to which the Data Holder may have access in that context shall be treated as confidential.]

[Comment: this section 2.10 is mainly relevant in case strict restrictions on use are selected, in order to allow the Data Holder to verify compliance with such restrictions. It can typically be removed in case no restrictions on use are selected by the parties.]

DSD addition: Any such audit shall be proportionate, limited to verifying compliance with this Agreement, and conducted in a manner that minimizes operational disruption and respects confidentiality, including any DSD-related obligations.

[Note: this adds proportionality and purpose-limitation to the audit's scope.]

3. ADDITIONAL SERVICES

3.1 Services. [Alt.1] In addition to the access to the Covered Data, the Data Holder may provide additional services to the Data Recipient. [Alt.2] The parties acknowledge that no additional services shall be rendered by the Data Holder, who offers no warranty of continuous availability nor of continuous access to the Covered Data and does not provide any support to the Data Recipient.

[Comment: Select Alt.1 if the Data Holder is also offering additional services (e.g. support, analysis, etc.) or Alt.2 if no additional services are contemplated.]

DSD Additions (compatible with either Alternative):

If the Data Holder provides additional services, it shall do so in a manner that:

- a) offers clear and accessible explanations of the methodologies, tools, and processes used;
- b) avoids creating unintended inferences about individuals, groups, or communities represented in the Covered Data;
- c) allows the Data Recipient to understand any limitations or uncertainties associated with the services;
- d) supports the safe and context-appropriate use of the Covered Data in accordance with the principles of Digital Self-Determination.

[Note: These additions anchor the services in transparency and responsible use but do not create new obligations of performance.]

3.2 Additional Terms. Any additional services or tools that may be offered to the Data Recipient shall be governed by additional terms, whether in the form of an API license agreement, terms of use of a platform or any services agreement that may be entered into by the parties.

DSD Additions:

The Data Holder shall ensure that such additional terms:

- a) are made available in clear and accessible language,
- b) describe any limits, risks, or context assumptions relevant to the additional services, and
- c) include a point of contact for questions concerning responsible use, data limitations, or potential Context Changes.

[Note: ensures that add-on tools cannot undermine the DSD alignment of the main contract.]

3.3 Interoperability. The Parties shall use their best efforts to facilitate the Interoperability of Covered Data, data sharing mechanisms and data services, if any, as follows:

- a) the dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the Data Recipient to find, access and use the Covered Data;
- b) the data structures, formats, vocabularies, classification schemes, taxonomies and code lists shall be sufficiently described in a consistent manner;
- c) the technical means to access the Covered Data, such as any API, and their terms of use and quality of service, shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;
- d) the means to enable the interoperability of smart contracts, if any, within their services and activities shall be provided.

[Drafting comment: this section 3.3 reflects the interoperability essential requirements under art. 28 of the Data Act, but on a best-efforts basis.]

DSD Enhancements to Interoperability (Important)

To support DSD, the Parties shall also:

- e) ensure that metadata and documentation are provided in a manner understandable to non-technical stakeholders where appropriate;
- f) avoid implementing interoperability in a way that creates new risks of inappropriate inference or re-identification, including risks affecting identifiable groups or communities;
- g) notify the other Party if interoperability features introduce or reveal any new Context Change, limitations, or potential Harm or Misalignment, and suspend the relevant functionality until mitigations are agreed.

(Note: This ties the Interoperability clause to governance and responsible risk mitigation, not just technical compatibility.)

4. ATTRIBUTION

[Alt.1] The origin of the Covered Data and identity of the Data Holder shall systematically be made available to third parties to whom the Covered Data and/or the Results have been Distributed. [Alt.2] The Data Recipient shall always seek prior written authorization from the Data Holder to mention the origin of the Covered Data and the identity of the Data Holder in case of authorized Distribution of the Covered Data and/or Results.

[Comment: select Alt.1 if the Data Holder wishes that its identity and the origin of the data be automatically communicated when such data is being distributed to third parties; select Alt.2 if the Data Holder wishes to check and confirm prior to the distribution whether its identity should be mentioned or not.]

DSD Enhancements (compatible with either alternative)

To support DSD and the responsible interpretation of the Covered Data:

a) Accuracy & Contextual Integrity

Any attribution shall be accompanied by a clear and accurate description of the nature, scope, limitations, and original context of the Covered Data, so that third parties do not misunderstand or misinterpret its meaning or purpose.

b) Group & Community Sensitivities

The Data Recipient shall refrain from attribution practices that may misrepresent, stereotype or negatively affect identifiable groups or communities reflected in the Covered Data, or that may imply endorsement or involvement by such groups where no such endorsement exists.

c) Restrictions Flow-Down

Where attribution is made, the Data Recipient shall also communicate any relevant Restrictions and use limitations attached to the Covered Data, unless the Data Holder instructs otherwise.

d) Attribution as Non-Endorsement

Unless expressly agreed by the Data Holder in writing, attribution of the Covered Data shall not be presented or implied as an endorsement, certification, or validation of the Results by the Data Holder or by any groups or communities represented in the Covered Data.

e) Context Change Notifications

If the Data Recipient becomes aware that attribution—whether in form or content—may create a Context Change or newly introduce potential Harm or Misalignment, it shall promptly notify the Data Holder and, where necessary, suspend such attribution until both Parties agree on mitigations.

5. SECURITY

5.1 IT Security. The Data Recipient shall comply with all laws and regulations applicable to the privacy or security of the Covered Data.

DSD Additions (practical and minimal):

The Data Recipient shall also implement security measures that are appropriate to the nature, sensitivity, and potential impacts of the Covered Data, including the potential for indirect impacts on individuals, groups, or communities represented in the Covered Data.

Such measures shall include, at minimum:

- a) access controls and authentication appropriate to the access modality;
- b) industry-standard technical and organizational measures to prevent unauthorized access, alteration, or misuse;
- c) safeguards to avoid inference, reconstruction, or linkage attacks that may create Harm or Misalignment;
- d) internal procedures that ensure the Covered Data is used only for the purposes permitted under this Agreement.

(Note: This aligns security with contextual integrity and group-level protection.)

5.2 Breach Monitoring. In the event of an actual or suspected security incident involving its information systems, the Data Recipient shall immediately notify the Data Holder and comply with any applicable notification obligations.

DSD Additions:

Upon becoming aware of an actual or suspected incident, the Data Recipient shall provide the Data Holder with:

- a) a brief description of the nature of the incident;
- b) an assessment of whether the incident may result in Harm or Misalignment;
- c) a description of immediate containment measures taken;
- d) follow-up actions planned to prevent recurrence.

Where the Covered Data relates to identifiable groups or communities, the Parties shall in good faith assess whether any **context-specific mitigations** or communication measures may be appropriate.

(Note: supports agency, transparency and harm mitigation, without introducing new statutory obligations.)

5.3 Suspension for Risk Mitigation (*new DSD clause*)

If either Party reasonably believes that continued access to or use of the Covered Data may create a material risk of Harm or Misalignment, including due to a security incident, inference vulnerability, or newly discovered dataset sensitivity, the concerned Party may temporarily suspend access or use of the Covered Data.

Such suspension shall be:

- a) promptly communicated to the other Party;
- b) limited to what is strictly necessary;
- c) reviewed jointly by the Parties in good faith to determine appropriate safeguards or conditions for resuming access.

(Note: key to dynamic governance and contextual integrity under DSD).

5.4 Security and Use Review Mechanism (*optional*)

Upon reasonable request, the Parties shall meet to review applicable security and governance measures to ensure continued alignment with:

- ▶ the permitted purposes of this Agreement,
- ▶ evolving best practices, and
- ▶ principles of Digital Self-Determination.

(Note: This is non-auditory, non-intrusive, and preserves the voluntary nature of the agreement.)

6. REPRESENTATIONS AND WARRANTIES

6.1 Each party represents that it will perform its obligations under this Agreement in compliance with applicable laws. In addition, each party shall act in good faith to ensure that its use of the Covered Data remains consistent with the principles of DSD, including transparency regarding the context and limitations of the Covered Data and the prevention of foreseeable Harm or Misalignment.

6.2 The Data Holder offers no warranty that the Data Recipient shall not be granted access to Personal Data in the performance of this Agreement and should the Data Recipient be granted access to Personal Data in the framework of this Agreement, the Data Recipient acknowledges that it may be subject to additional obligations to comply with privacy and data protection laws and commits to take the relevant measures to comply with such obligations, if any. The Data Recipient shall promptly notify the Data Holder if it becomes aware that the Covered Data contains, or could reasonably allow the inference of, Personal Data or sensitive group-level characteristics, so that the Parties may assess appropriate safeguards or limitations on use.

(Note: to connect privacy obligations with contextual and collective DSD risks).

6.3 The Covered Data is provided on an “as is” and “as available” basis, without warranties or conditions of any kind, either express or implied including, without limitation, any warranties or conditions of title, non-infringement, merchantability or fitness for a particular purpose. Both Parties acknowledge that the Covered Data may contain limitations, uncertainties or biases inherent to its collection or processing. The Parties shall cooperate in good faith to clarify any such issues if identified during the Term, in order to support responsible and context-appropriate use of the Covered Data.

(Note: clarifies DSD without implying data-quality warranties.)

6.4 Within the limits of applicable law, the Data Holder shall have no liability for any direct or indirect damages (including without limitation lost profits), however caused and on any theory of liability, whether in contract, strict liability, or civil liability (including negligence or otherwise) arising in any way out of the covered data, even if advised of the possibility of such damages. Nothing in this Section shall prevent either Party from raising concerns or requesting a review under this Agreement where it reasonably believes that continued use of the Covered Data may lead to Harm or Misalignment. Such review shall be handled through the governance mechanisms set forth in this Agreement and shall not be construed as an admission of liability.

(Note: preserves full limitation of liability while enabling DSD governance dialogue.)

7. DURATION AND TERMINATION

7.1 Duration. This Agreement enters into force on the date first written above and for the duration of the subscription term mentioned on the cover sheet. It shall be automatically renewed, at the same conditions, for additional terms of the same duration unless terminated in accordance with this Agreement. The initial subscription term and all renewal terms shall together constitute the Term. During each renewal, the Parties may, upon request, review whether the context of use or the sensitivity of the Covered Data has materially changed and whether additional safeguards or adjustments are appropriate.

(Note: this adds an optional governance review without creating an obligation.)

7.2 Voluntary Termination. Each party may terminate this Agreement without cause with a Termination Notice as set forth on the cover sheet. Upon voluntary termination by either Party, the Parties shall cooperate in good faith to ensure a responsible wind-down of any ongoing uses of the Covered Data that might affect identifiable groups or communities, consistent with the principles of Digital Self-Determination.

(Note: adds a soft governance duty, not a performance or service obligation.)

7.3 Automatic Termination. This Agreement shall automatically terminate in case of breach of any of the terms and conditions of this Agreement by the Data Recipient or a Downward Recipient. **(DSD Addition):** For the avoidance of doubt: a) an automatic termination shall not require prior notification where the breach presents a material risk of Harm or Misalignment; b) where the breach does not present such risk, the Data Holder may, but is not obliged to, provide an opportunity to cure the breach before termination.

(Note: preserves the Data Holder’s discretion and adds DSD aligned language about harmful uses.)

7.4 Effect of Termination. Upon termination of this Agreement for any reason whatsoever, the Data Recipient shall no longer be granted access to the Covered Data nor be authorized to make any use of the Covered Data. The Data Recipient shall remain entitled to use the Results and sections 2.8, 4, 6.4 and 8 shall survive the termination of this Agreement.

DSD Additions:

The Data Recipient shall, upon termination:

- a) delete, return, or render inaccessible any Covered Data in its possession, except where expressly required by law to retain it;
- b) refrain from any further use of the Covered Data, including uses that could reasonably lead to Harm or Misalignment;
- c) retain the Results only to the extent that the Results do not enable reconstruction, reverse engineering, or inference of the Covered Data;
- d) document any outstanding issues that may be relevant to the Data Holder’s assessment of risks or to future contextual integrity.

(Note: This ensures responsible wind-down, preserves Result rights, and prevents misuse after termination.)

8. MISCELLANEOUS

8.1 Entire Agreement. This Agreement contains all of the terms and conditions agreed upon by the parties relating to its subject matter and supersedes all prior agreements, negotiations, correspondence, undertakings and communications of the parties, whether oral or written, with respect to such subject matter. The Parties acknowledge that governance mechanisms relating to Digital Self-Determination, Context Changes, and prevention of Harm or Misalignment are integral to the interpretation and implementation of this Agreement.

8.2 Form. Any reference to the written form in this Agreement, and any reference to any notice or document to be delivered in writing, shall be deemed to be satisfied by email or any form of electronic signature service such as PDF or DocuSign. Notices relating to concerns regarding DSD, Harm, Misalignment, or Context Change shall be sent to the Data Steward or to another designated point of contact identified by each Party.

(Note: This operationalizes the Data Steward and ensures governance notices don't get lost.)

8.3 Severability. If any provision of this Agreement is held to be unenforceable for any reason, it shall be adjusted rather than voided, if possible, in order to achieve the intent of the parties to the fullest extent possible. In any event, all other provisions of this Agreement shall remain valid and enforceable to the fullest extent possible. In adjusting any unenforceable provision, the Parties shall consider how the adjusted provision can continue to support the principles of Digital Self-Determination and maintain the Agreement's overall governance structure.

(Note: Soft; no legal risk; ensures DSD does not disappear if one clause is invalid.)

8.4 No Waiver. The failure of any of the parties to enforce any of the provisions of this Agreement or any rights with respect thereto shall in no way be considered as a waiver of such provisions or rights or in any way affect the validity of this Agreement. The waiver of any breach of this Agreement by any party shall not be construed as a waiver of any other prior or subsequent breach. A Party's decision not to invoke a governance mechanism or raise a DSD-related concern at any specific time shall not be construed as a waiver of its right to do so later.

(Note: avoids "you didn't raise the risk earlier, so you waived it.")

8.5 Governing Law. This Agreement shall be governed by and construed in accordance with Swiss substantive law, without reference to its conflict of laws provisions.

Nothing in this Section prevents the Parties from considering relevant international soft-law frameworks concerning Digital Self-Determination, responsible data use, or data governance where helpful to interpret the context or intent of specific provisions of this Agreement.

8.6 Jurisdiction. [Alt.1] Any dispute, controversy or claim arising out of or in relation with this Agreement shall be submitted to the ordinary courts at the domicile or the registered seat of the Data Holder, subject to appeal to the competent superior authority. [Alt.2] Any dispute, controversy or claim arising out of or in relation with this Agreement shall be resolved by arbitration in accordance with the Swiss Rules of International Arbitration of the Swiss Arbitration Centre and the ITDR—Institution for IT and Data Dispute Resolution Recommendations for Arbitration, both in force on the date on which the Notice of Arbitration is submitted in accordance with these Rules and Recommendations. The number of arbitrators

shall be one or three. The seat of the arbitration shall be the seat of the Data Holder. The arbitral proceedings shall be conducted in English. Notwithstanding the above, the parties may agree at any time to submit the dispute to mediation in accordance with the Swiss Rules of Mediation of the Swiss Arbitration Centre and the ITDR – Institution for IT and Data Dispute Resolution Recommendations for Mediation, both in force on the date on which the request for mediation is submitted in accordance with these Rules and Recommendations. Notwithstanding the above, the parties may agree at any time prior to submitting the dispute to arbitration or mediation to submit the dispute to assessment by an expert opinion in accordance with the ITDR – Institution for IT and Data Dispute Resolution Rules of Procedure for Expert Opinions in force on the date on which the request for assessment by an expert opinion is submitted in accordance with these Rules.

[Comment: select Alt.1 if the parties wish to subject potential disputes relating to the agreement to ordinary Swiss courts, without a specific expertise in the field; this corresponds to the ordinary route in case of disputes; select Alt. 2 if the parties wish to subject potential disputes to arbitration by experts in the field, as well as benefit from the ability to ask an expert to intervene before initiating an arbitration or mediation.]

DSD Addition (applies to both alternatives):

Prior to initiating litigation, arbitration, mediation or expert proceedings, the Parties shall meet in good faith, unless the circumstances make such meeting impossible, to determine whether the dispute relates in whole or in part to a Context Change, Harm, Misalignment or other DSD governance issue and whether it may be resolved through the collaborative mechanisms set out in this Agreement.

(Note: This is procedural, non-binding, and aligns dispute resolution with DSD governance.)

Data Holder

Data Recipient



A ROADMAP FOR
DIGITAL SELF-DETERMINATION
IN DATA SPACES