Intersection of Provenance and the AI Act

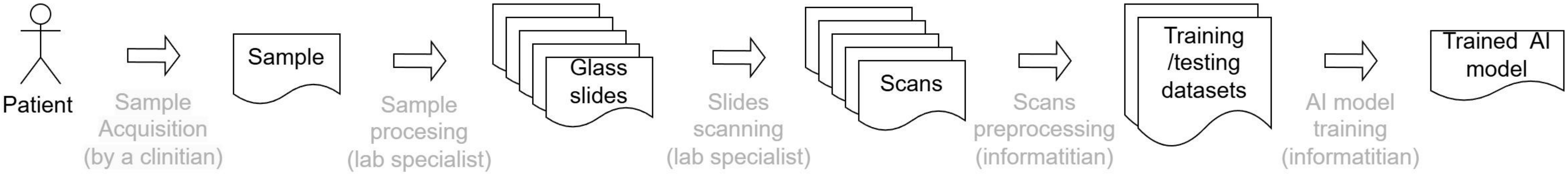
And how it relates to OS II

What’s Provenance?

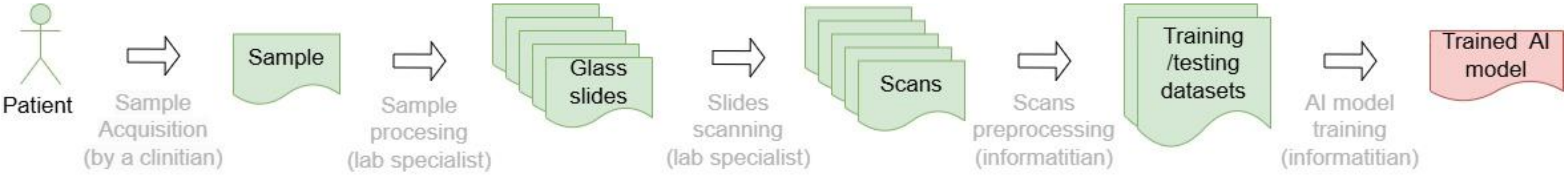
Provenance

“Information that documents ***the history*** *of* ***a described object*** *and related* ***described activities****, including information about* ***origin or source*** *of the described object,* ***any changes*** *that may have taken place since it was originated, and* ***who has had custody*** *of it since it was originated.”*

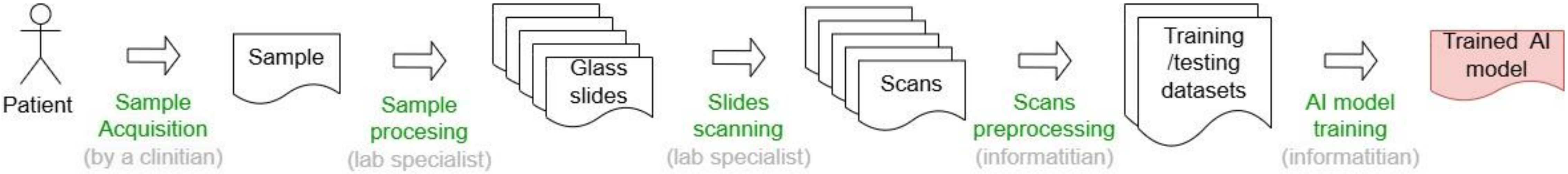
Provenance


Patient
Sample Acquisition (by a clinitian)
Sample
Sample procesing (lab specialist)
Glass slides
Slides scanning (lab specialist)
Scans
Scans preprocessing (informatitian)
Training /testing datasets
AI model training (informatitian)
Trained AI model

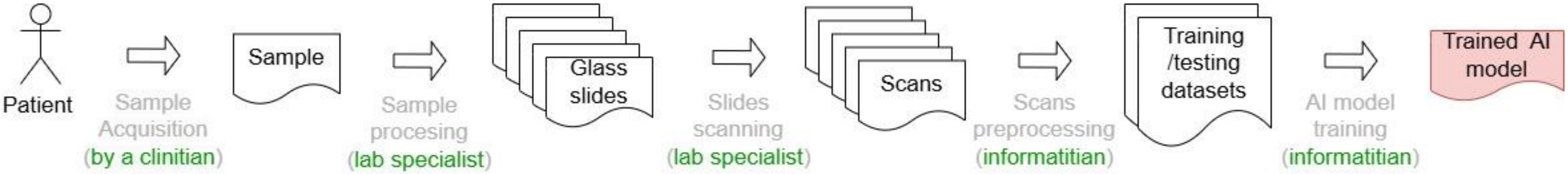
Provenance – origin or source


Patient
Sample Acquisition (by a clinitian)
Sample
Sample procesing (lab specialist)
Glass slides
Slides scanning (lab specialist)
Scans
Scans preprocessing (informatitian)
Training /testing datasets
AI model training (informatitian)
Trained AI model

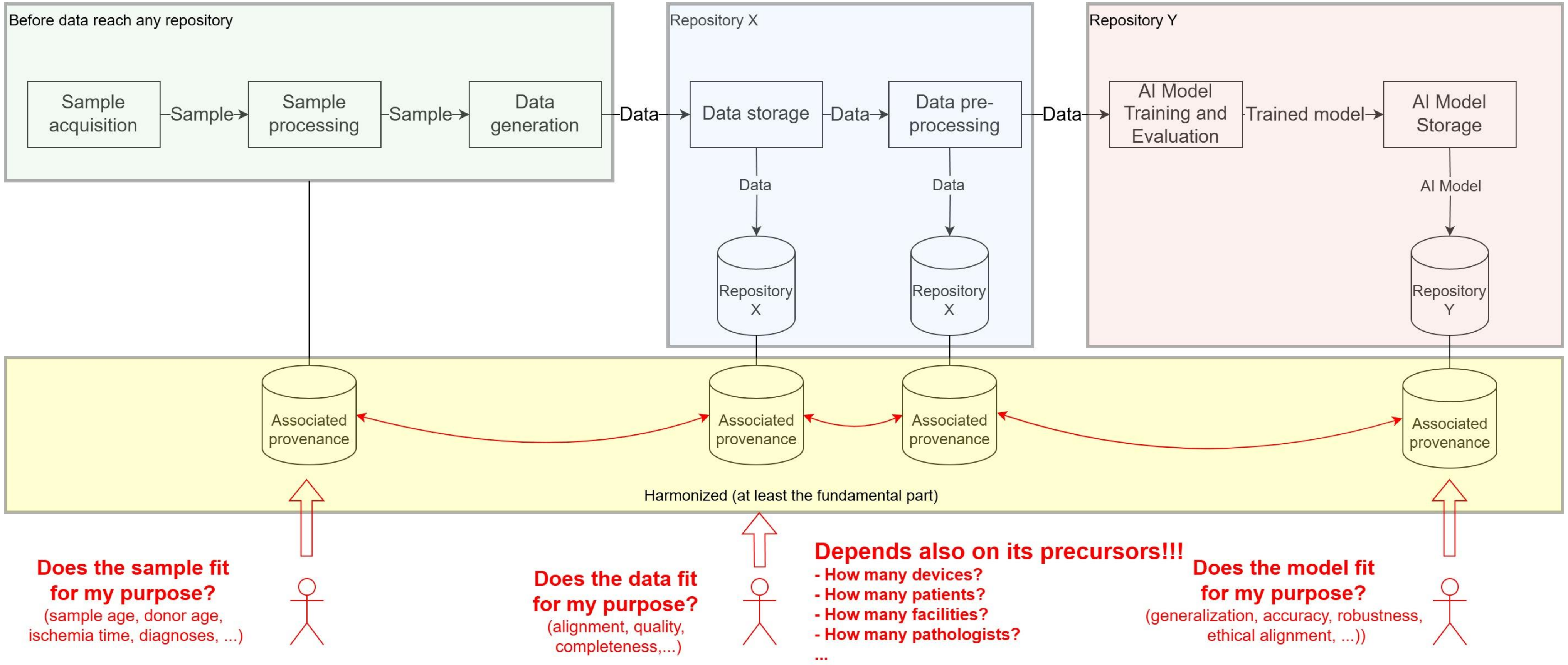
Provenance – changes



Provenance – custody



Long-term Vision



Before data reach any repository

Sample acquisition → Sample → Sample processing → Sample → Data generation → Data →

Repository X

Data storage → Data → Data pre-processing → Data →

Data storage → Data → Repository X

Data pre-processing → Data → Repository X

Repository Y

AI Model Training and Evaluation → Trained model → AI Model Storage

AI Model Storage → AI Model → Repository Y

Associated provenance ↔ Associated provenance ↔ Associated provenance ↔ Associated provenance

Harmonized (at least the fundamental part)

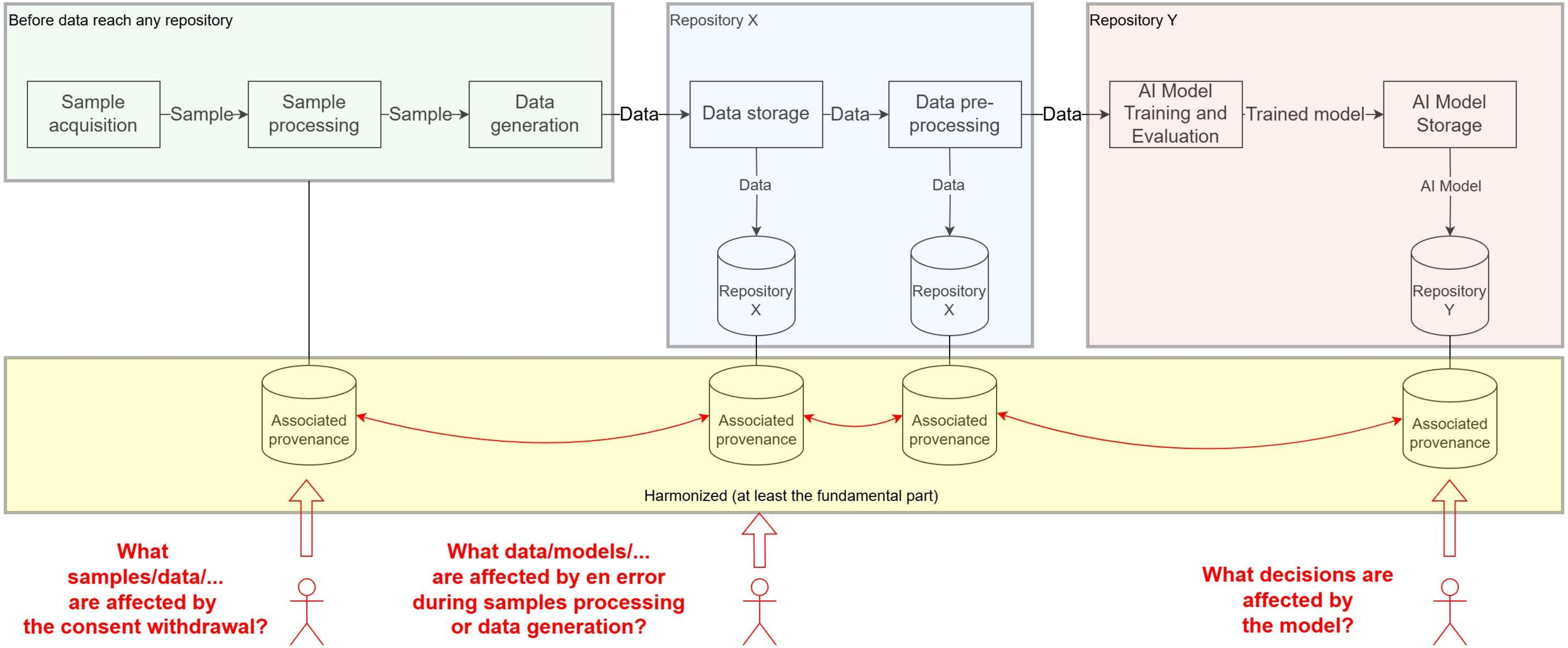
Does the sample fit for my purpose?
(sample age, donor age, ischemia time, diagnoses, ...)

Does the data fit for my purpose?
(alignment, quality, completeness,...)

Depends also on its precursors!!!
- **How many devices?**
- **How many patients?**
- **How many facilities?**
- **How many pathologists?**
...

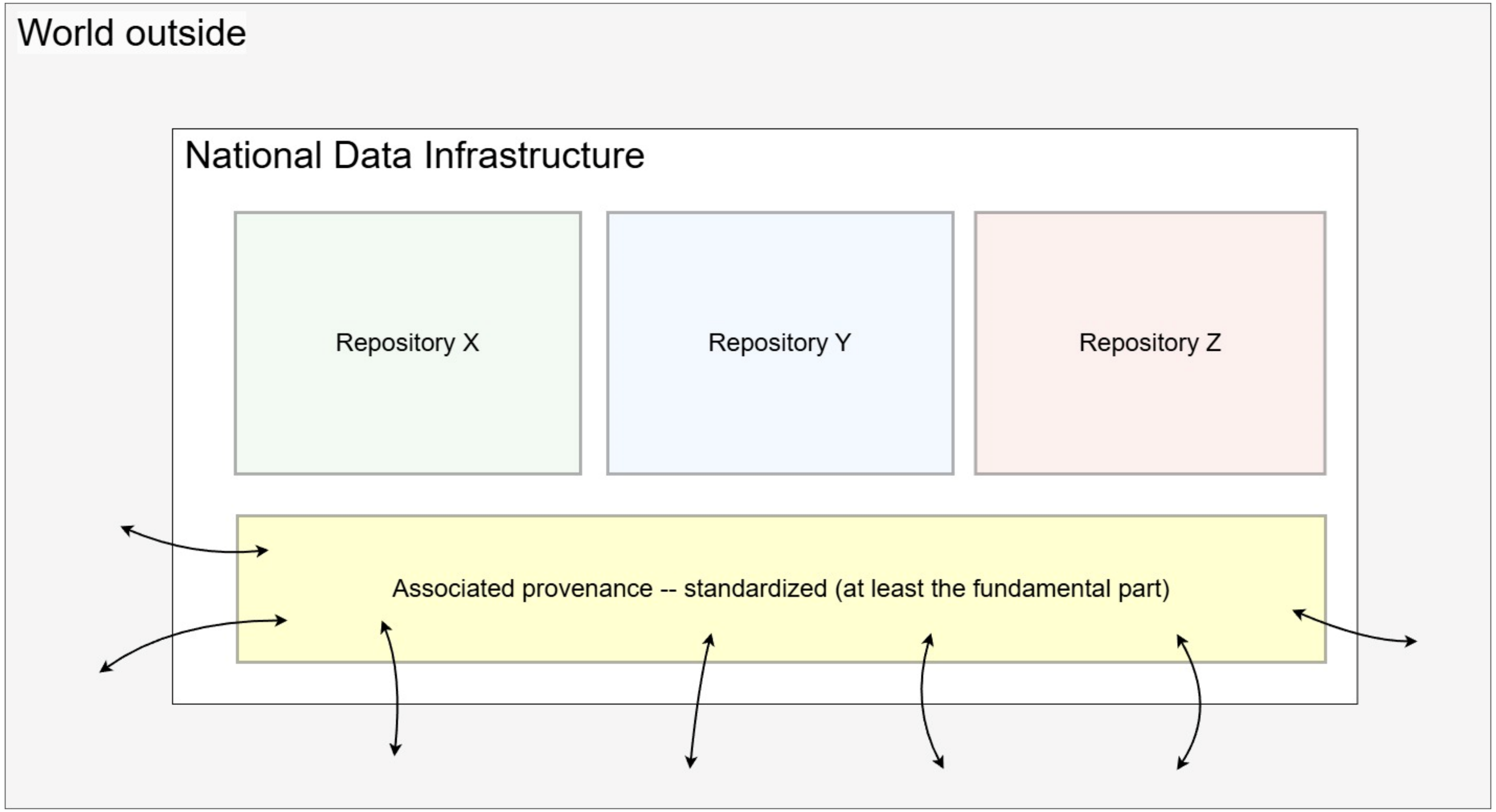
Does the model fit for my purpose?
(generalization, accuracy, robustness, ethical alignment, ...))

Long-term Vision



Before data reach any repository
Sample acquisition
Sample
Sample processing
Sample
Data generation
Data
Repository X
Data storage
Data
Data pre-processing
Data
Data
Data
Repository X
Repository X
Repository Y
AI Model Training and Evaluation
Trained model
AI Model Storage
AI Model
Repository Y
Associated provenance
Associated provenance
Associated provenance
Associated provenance
Harmonized (at least the fundamental part)
What samples/data/... are affected by the consent withdrawal?
What data/models/... are affected by en error during samples processing or data generation?
What decisions are affected by the model?

Long-term Vision


World outside
National Data Infrastructure
Repository X
Repository Y
Repository Z
Associated provenance -- standardized (at least the fundamental part)

What’s the AI Act?

AI Act

- A regulation setting harmonized rules on AI in EU
- Fostering trustworthy AI
  - AI systems respect fundamental rights, safety, and ethical principles
- Risk based approach to classify AI systems into four categories
- Timeline
  - August 2024 – publication
  - August 2025 – appointment of national authorities for enforcing the regulation
  - August 2026 – starts applying to high-risk systems
  - August 2027 – starts applying to all risk categories

The AI Act and Provenance

Article 11: Technical Documentation (of High-Risk AI System)

*“The **technical documentation of a high-risk AI** system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date…It shall contain, at a minimum, the elements set out in **Annex IV**.”*

Article 53: Obligations for Providers of General-Purpose AI Models

“Providers of general-purpose AI models shall: (a) draw up and keep up-to-date the ***technical documentation of the model****, including its training and testing process and the results of its evaluation, which shall contain, at a minimum, the information set out in* ***Annex XI*** *for the purpose of providing it, upon request,* ***to the AI Office and the national competent authorities.****”*

Article 53: Obligations for Providers of General-Purpose AI Models

"Providers of general-purpose AI models shall: (b) draw up, keep up-to-date and make available ***information and documentation to providers of AI systems*** *who intend to integrate the general-purpose AI model into their AI systems…documentation shall: ii) contain, at a minimum, the elements set out in* ***Annex XII****"*

The Annex IV

"...including a general description of these data sets, ***information about their provenance****, scope and main characteristics;* ***how the data was obtained and selected****..."*

The Annex XI

“… information on the data used for training, testing and validation, where applicable, including the type and ***provenance of data*** *and* ***curation methodologies*** *(e.g. cleaning, filtering etc.), the number of data points, their scope and main characteristics;* ***how the data was obtained and selected*** *as well as all other measures to detect the unsuitability of data sources and methods to detect identifiable biases, where applicable…”*

The Annex XI

“…information on the data used for training, testing and validation, where applicable, including the type and ***provenance of data*** *and curation methodologies…”*

AI Act

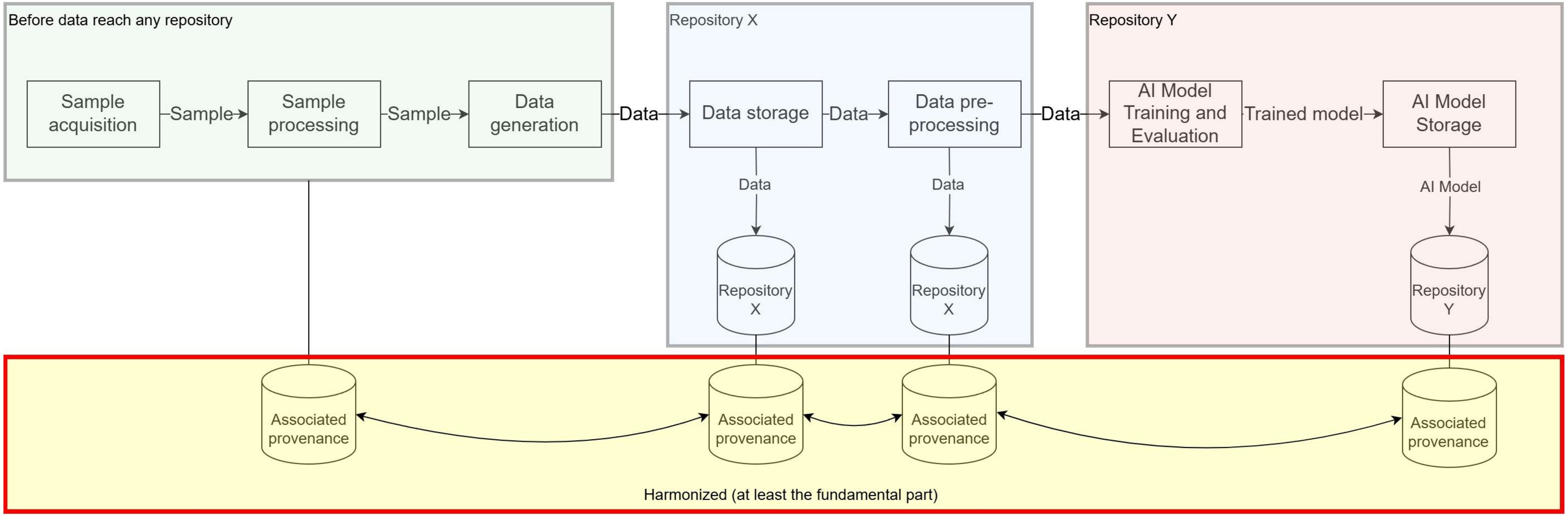
- European Commission request to
  - CEN -- European Committee for Standardization
  - CENELEC -- European Committee for Electrotechnical Standardization
- To develop Harmonized Standards supporting the compliance with AI Act
  - Based on existing standards (link)
- Standards to be delivered by April 2025
- Aim to clarify technical and operational requirements
- Adherence to the Harmonized Standards == compliance with AI Act requirements

Potential requirements

- Independence of test dataset and other datasets used in the design/development of an AI system
  - E.g., individual’s samples can not be included in both training and testing datasets
  - People who have participated in the design/development of the AI system can not choose, collect, or annotate the data
- System designed/developed/tested using data of the locals in which it will be deployed
- Origin of the algorithms and modifications

Provenance výstupy v OS II

Horizontálne výstupy



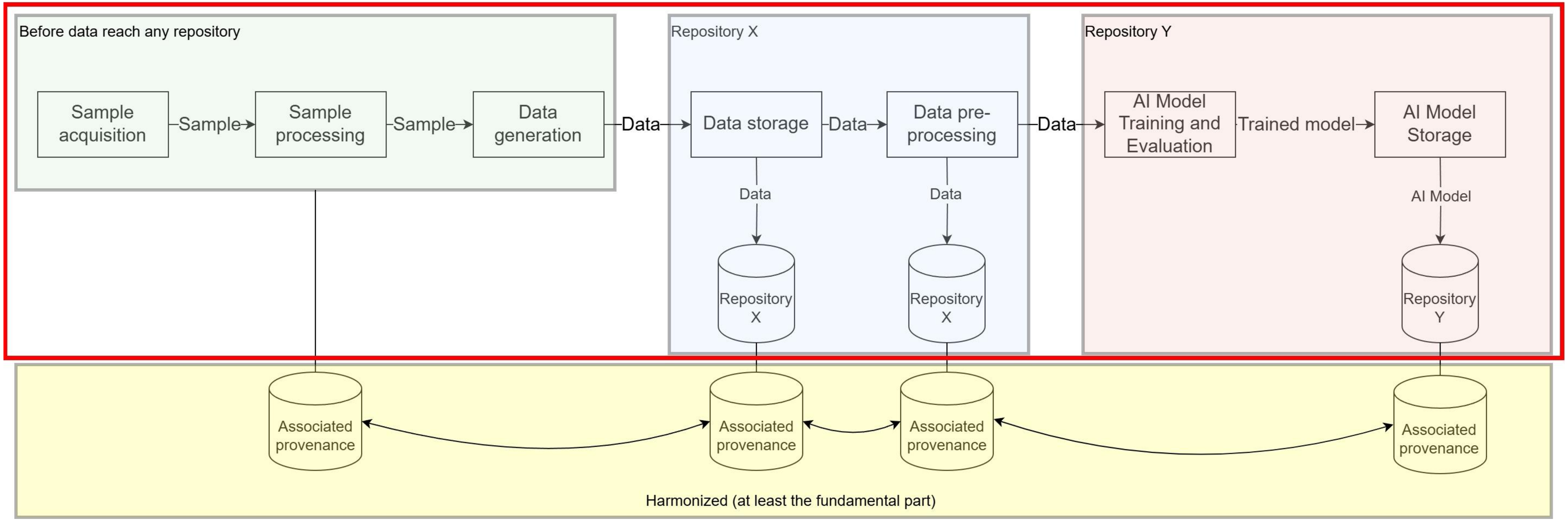
Horizontálne výstupy

- Hlavný partner: MUNI
- Budget: Horizontálna kľúčová aktivita
- Zahŕňa
  - Vývoj všeobecných nástrojov integrovateľných s repozitárovvou platformou/výskumným prostredím
    - Nástroje pre prístup, uloženie, validácia vstupu, generovanie meta informácie, prehľadávanie
  - Vývoj realizovaný na konkrétnych use cases (RationAI/BiomedAI MUNI (+ďalšie MUNI?))
  - Demonštrácia integrácie technologického riešenia s konkrétnou inštanciou repozitára
    - Možné hodnotiť áno/nie
  - Podpora integrácie technologického riešenia s konkrétnymi inštanciami repozitárov
  - Napojenie na AAI
  - Napojenie na základný metadatový model (a NMA)

Horizontálne výstupy

- Ďalej zahŕňa
  - Vedenie, koordinácia, zarovnanie s ďalšími aktivitami
    - Vertikálne provenance aktivity (viď. ďalej)
    - Iné kľúčové aktivity (napr. oborové aktivity)
  - Interakcia so súvisiacimi projektmi
  - Licencie
  - Podklady pre školiace aktivity a povedomie
  - Metodika pre prácu s provenance v NDI

Vertikálne aktivity



Vertikálne výstupy – Analýza

- Budget: Tématické kľúčové aktivity
- Prakticky:
  - Aké všetky informácie budú potrebné?
  - Aké informácie sú zachytené a ktoré informácie chýbajú?
- Výstup
  - Dokument popisujúci potrebné informácie pre konkrétne procesy v repozitári (prípadne pred repozitárom) + návrch architektúry pre integráciu s horizontálnymi výstupmi
- ~3-6 PMs (analytik) v závislosti na komplexite daného use case
  - Možný prienik s doménovými metadatovými modelmi

Vertikálne výstupy – Integrácia

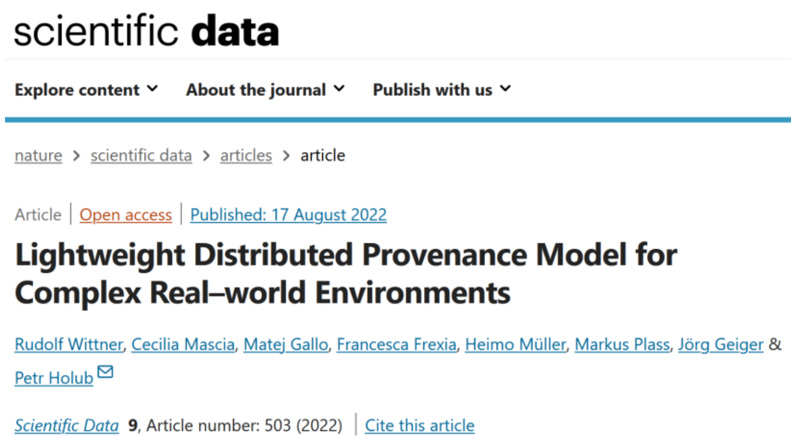
- Budget: Tématické kľúčové aktivity
- Technická integrácia výstupov horizotnálnej aktivity s konkrétnou inštanciou repozitára (/ELNs/...)
- Zahŕňa
  - Rozšírenie zdrojového systému v prípade doplnenia chýbajúcich informácií
  - Návrh reprezentácie informácií zo zdrojového systému pomocou harmonizovaného dátového modelu pre reprezentáciu provenance (W3C PROV, CPM, ISO 23494)
  - Implementácia transformácie informácií zo zdrojového systému
    - Využitie nástrojov implementovaných v rámci horizontálnej aktivity
    - Možné hodnotiť áno/nie
- ~6-18 PMs (programátor + admin) v závislosti na komplexite daného systému

Súvislosť s medzinárodnými aktivitami

- Priama väzba na európske projekty:
  - EOSC-Life (CPM+ISO 23494)
  - BY-COVID (revízia CPM+ISO 23494)
  - EvolveBBMRI (adoptovanie CPM+ISO 23494 v BBMRI-ERIC)
- Väzba na aktivity výzkumných infrašturktúr
  - BBMRI-ERIC
  - (EMBRC – zapojenie do EOSC-Life)
- Väzba na medzinárodné iniciatívy
  - RO-Crates (ELIXIR)

Related Publications

- **Wittner R, Mascia C, Gallo M, Frexia F, Müller H, Plass M, Geiger J, Holub P. 2022. Lightweight distributed provenance model for complex real–world environments. *Scientific Data*, 9(1), p.503.**
- **Plas M, Wittner R, Holub P, Frexia F, Mascia C, Gallo M, Müller H, Geiger J. 2023. Provenance of specimen and data–A prerequisite for AI development in computational pathology. *New Biotechnology*, 78, pp.22-28.**
- Fairweather E, Wittner R, Chapman M, Holub P, Curcin V. 2020, June. Non-repudiable provenance for clinical decision support systems. In *International Provenance and Annotation Workshop* (pp. 165-182). Cham: Springer International Publishing.
- Wittner R, Holub P, Mascia C, et al. 2023. Toward a common standard for data and specimen provenance in life sciences. *Learning Health Systems*, p.e10365.
- Leo S, Crusoe MR, Rodríguez-Navas L, Sirvent R, Kanitz A, et al. 2024. Recording provenance of workflow runs with RO-Crate. PLOS ONE 19(9): e0309210.



scientific **data**

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › scientific data › articles › article

Article | Open access | Published: 17 August 2022

Lightweight Distributed Provenance Model for Complex Real–world Environments

Rudolf Wittner, Cecilia Mascia, Matej Gallo, Francesca Frexia, Heimo Müller, Markus Plass, Jörg Geiger & Petr Holub

Scientific Data **9**, Article number: 503 (2022) | Cite this article

ELSEVIER

New Biotechnology

Volume 78, 25 December 2023, Pages 22-28

Provenance of specimen and data – A prerequisite for AI development in computational pathology

Markus Plass [a], Rudolf Wittner [b], Petr Holub [b], Francesca Frexia [c], Cecilia Mascia [c], Matej Gallo [b], Heimo Müller [a], Jörg Geiger [d]

Learning Health Systems

Open Access

COMMENTARY | Open Access

Toward a common standard for data and specimen provenance in life sciences

Rudolf Wittner, Petr Holub, Cecilia Mascia, Francesca Frexia, Heimo Müller, Markus Plass, Clare Allocca, Fay Betsou, Tony Burdett, Ibon Cancio, Adriane Chapman, Martin Chapman, Mélanie Courtot, Vasa Curcin, Johann Eder, Mark Elliot, Katrina Exter, Carole Goble, Martin Golebiewski, Bron Kisler, Andreas Kremer, Simone Leo, Sheng Lin-Gibson, Anna Marsano, Marco Mattavelli, Josh Moore, Hiroki Nakae, Isabelle Perseil, Ayat Salman, James Sluka, Stian Soiland-Reyes, Caterina Strambio-De-Castillia, Michael Sussman, Jason R. Swedlow, Kurt Zatloukal, Jörg Geiger

... See fewer authors ^

First published: 18 April 2023 | https://doi.org/10.1002/lrh2.10365