Data access for AI & ML

Demystifying the regulatory landscape

DATA PRIVACY | INDUSTRY | AI

A small sample of the expanding regulations

Common areas are emerging

Data residency

Governance

Security

Privacy

Consent, transparency, & purpose

Clear and explicit consent before data collection, informing about data use, purpose, and third-party sharing.

Individual data rights

Right to access, rectification, erasure, and limitations on automated decision making.

Data integrity & quality

Data minimization – collect only what's necessary – and ensure data is accurate and up-to-date.

Protection & security

Implement robust security measures, preserve the integrity and consistency of data.

Governance & accountability

Demonstrate compliance with regulations, internal data protection policies, assessments and organizational measures.

Ethical & responsible use

Ethical and responsible use of data in AI and automated systems, with stricter requirements for sensitive data such as health or financial data.

New opportunities are already here...

Commercializing data for ML unlocks business value

Foundation models make AI more accessible than ever

Data is unlocked to solve business, societal, and global challenges

New challenges are appearing...

Privacy risks resulting from efforts to monetize data[1]

Balancing localization requirements with business needs[1]

Immaturity in managing privacy through use of AI[2]

Model-memory results in data privacy breaches

No major foundational model providers comply with the proposed EU AI Act[2]

Compliance risks already exist...

1801
fines issued under GDPR (as of August 2023)[3]

4.45MUSD
the global average cost of a data breach in 2023[4]

692
large healthcare data breaches have been reported[5]

Navigate the regulatory landscape

1. **Data security** to safeguard against breaches or unauthorized access
2. **Permitted data access** and use complies with consent
3. **Data residency requirements** are met and data transfer complexities avoided
4. **Activity is monitored and audited** to ensure it's being used as intended
5. **Requirements around transparency, bias, and fairness** are met through use of real-world, representative data

APHERIS

Federated computational governance for private, secure ML

Federation

Keep data local to meet data residency and sovereignty requirements. Send computations to data to avoid sharing.

Federation – don't move data

Governance

Set and audit asset policies that ensure security and data privacy at the computational level. Revoke policies at any time.

Governance Portal – stay in control of who does what with your data

Security

Access controls and permissions ensure only allowed computations run on data. Log activity for traceability.

Trust Center – best practice for compliance with regulation

Privacy

Apply privacy techniques according to your requirements. Review and approve or reject compute jobs to ensure compliance.

Model Registry – categorized model cards provide a privacy and security evaluation

Built to successfully balance innovation and compliance

Data stays local to meet residency requirements. Provision only necessary data to meet data minimization.

Define and set asset policies to control what can be run on your data. Revoke policies at any time.

Audit and trace all activity on your data to meet traceability requirements.

Inspect compute requests and approve what is run on your data in accordance with compliance obligations.

Ensure data security with encryption at rest and in-transit, no ingress, and role-based access control.

Only privacy-preserving results are returned by employing the right privacy controls and to avoid models being subject to data privacy regulation.

Ready to delve deeper into compliant computational access to data?

apheris.com
info@apheris.com

APHERIS

References

1 - Privacy Risk Study 2023
2 - Do Foundation Model Providers Comply with the Draft EU AI Act?
3 - Enforcement tracker
4 - Cost of a Data Breach Report 2023
5 - June 2022 Healthcare Data Breach Report