GLOBAL DATA PROTECTION POLICY

Fluidra Group

Global Internal Audit & Compliance Department

Approved by the Board of Directors on May 4th, 2026

FLUIDRA

Document information

Title	Global Data Protection Policy
Category	Policy
Description	To establish a structured data protection compliance framework that ensures the company manages personal data according to international regulations and best practices. This framework defines the principles that all levels of Fluidra must follow regarding data protection.
Scope	Applicable to all Fluidra companies where Fluidra operates ("FLUIDRA").
Sponsor	Global Internal Audit & Compliance Department
Effective date	May 4th, 2026
Version	1.0
Last review date	May 4th, 2026

Index

1. Introduction

At Fluidra, respecting the privacy of individuals and protecting personal data is fundamental to how we operate. Across all regions where we do business, we are committed to complying with applicable data protection laws—whether under the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) and other U.S. state laws, or equivalent national frameworks in Australia, Latin America, and beyond. Fluidra's Global Data Protection Policy ("the Policy") applies globally to all Fluidra operations and Sites. We are guided by international privacy principles—including those found in the GDPR, CCPA/CPRA, and other frameworks—while recognizing that local laws and regulatory expectations vary across jurisdictions. Our goal is to implement consistent and risk-appropriate privacy practices that meet or exceed local legal requirements.

However, for certain regions, products, or services, specific privacy notices may apply instead of, or in addition to, this Policy. In case of a conflict between this Policy and local data protection laws, the applicable local law shall take precedence. This Policy is intended to guide internal compliance efforts and does not confer legal rights to third parties.

Personal data (or **personal information**) is defined under the specific applicable data protection law and broadly refers to any information that identifies, or can reasonably be used to identify, an individual. This includes basic details like name, email or phone number, as well as data such as salary, performance data, working hours, voice, image or IP address. Even in B2B relationships, data processing often involves identifiable individuals. All these types of data must be handled with care and protected appropriately, pursuant to the relevant regulatory framework. Terminology may vary by jurisdiction. For example, "personal data" (under GDPR) and "personal information" (under CCPA) refer to conceptually similar categories of information, subject to the specific definitions in each applicable law.

Processing activities cover a wide range of actions involving personal data, such as accessing, anonymizing, collecting, recording, storing, using, analysing, combining, sharing or deleting it.

At Fluidra, the most common processing of personal data involves the following groups of **data subjects:**

- Employees and Candidates
- VIPs and Executives
- Customers B2B and B2C (including IoT users)
- Leads
- Suppliers (business contacts)
- Investors
- Visitors

2. Scope of application, purpose & objectives

This Policy is part of Fluidra's global compliance framework and is consistent with its Code of Ethics. It reflects Fluidra's commitment to handling personal data responsibly and in line with applicable laws, including GDPR, CCPA and the Australian Privacy Act. Accordingly, the level of compliance will reflect applicable legal requirements in each jurisdiction, supported by proportional safeguards tailored to the nature of the product, service, and regulatory environment. Where feasible and appropriate, Fluidra will draw upon leading global standards to promote consistency.

It applies to all entities and employees of the Fluidra Group, as well as any third parties acting on its behalf.

This Policy complements and supplements, but does not replace, certain local Privacy Policies and notices pursuant to local regulations.

FLUIDRA is committed to:

- Developing a consistent data protection and privacy framework across all of jurisdictions in which it operates; and
- Complying with the standard of care required by relevant law in all data handling practices.

This Policy is supported by internal procedures and guidelines that define the human, organizational, technological, and documentary measures in place to protect personal data and manage privacy risks effectively.

The ultimate goal of the Policy is to support the business in achieving its objectives ethically and lawfully, while minimizing privacy risks and ensuring compliance in the regions where Fluidra operates.

3. Principles of Data Protection

FLUIDRA's data protection strategy is based on the following key principles:

Lawfulness: Personal data shall be processed only where permitted or required by applicable law. In some regions (such as the EU), this may require a defined legal basis (e.g., consent or legitimate interest). In others (such as the United States), this may involve providing notice and a right to opt out of certain processing.

Transparency: Individuals must be clearly informed, consistent with local regulations, about how and why their personal data is processed.

Fairness: Personal data must not be processed in ways that are misleading or incompatible with what has been communicated to the individual.

Purpose limitation: Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes.

Data minimization: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This principle is closely linked to the principles of necessity and proportionality, particularly in the context of risk and impact assessments.

Accuracy: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be corrected or deleted without delay.

Storage limitation: Personal data shall be retained only for as long as necessary to fulfil the purposes for which it was collected and to comply with legal obligations, in line with applicable retention policies.

Integrity and security: Personal data must be processed securely, using appropriate technical and organisational measures to protect against unauthorised access, loss, alteration, or disclosure. Only authorised personnel may access Personal Information, and it must be collected and shared consistent with local regulation.

Accountability (proactive responsibility): FLUIDRA is responsible for ensuring compliance and must be able to demonstrate that local data protection requirements are met.

Data protection by design and by default: Privacy and data protection must be embedded from the outset in the design of any new process, service or product. An initial assessment shall be carried out to ensure that personal data is adequately protected throughout its lifecycle.

Cross-Border Transfers: Fluidra is committed to ensuring that personal data transferred across borders is handled in accordance with applicable data transfer requirements, including appropriate safeguards where required, such as standard contractual clauses or legally recognized alternatives.

These principles form the foundation of FLUIDRA's global approach to the responsible processing of personal data.

4. Governance and responsibilities in Data Protection

Board of Directors, Global Director of Internal Audit, Compliance Officer & Data Protection Officer

The Board of Directors, through the Audit Committee, is responsible for overseeing the effectiveness of the compliance model, including privacy and personal data protection.

In Europe and Australia, the Global Compliance Officer is also responsible for ensuring that the compliance model supports full adherence to data protection requirements in these regions. The Data Protection Officer (where appointed under applicable law) leads privacy governance from a data protection perspective and has indirect escalation to the Audit Committee on data protection matters.

In other regions, local leadership or designated privacy contacts are responsible for ensuring alignment with the Group's framework and local requirements.

Employees' Responsibilities

All Fluidra employees must comply with this Policy, any applicable local data protection policy, and the broader data protection framework. This includes:

- Understanding and applying applicable privacy policies, procedures, and guidelines.
- Staying informed about any updates or new requirements.
- Reporting any suspected data protection issues through the contact channels listed in Section 7.
- Participating in mandatory data protection training and awareness activities as appropriate to each employee's function, jurisdiction, and access to personal data.

5. Personal Data Protection business risks

The handling of personal data entails inherent business risks due to the sensitive nature of the information, the complexity and variability of applicable legal frameworks, and the significant penalties that may result from non-compliance. **These risks include, but are not limited to:**

- Administrative fines and sanctions imposed by regulatory authorities.
- Privacy violations (e.g. unlawful disclosure of personal data to third parties).
- Compensation claims by affected individuals or groups.
- Legal claims for damages resulting from privacy breaches, which may be adjudicated in courts across different jurisdictions.
- Reputational damage, loss of stakeholder trust, and negative media exposure.

These risks must be proactively identified, assessed, and mitigated through effective data protection measures. FLUIDRA is committed to maintaining high standards of data protection and expects all employees and collaborators to comply fully with the data protection framework in place. Adherence to these standards is essential for safeguarding personal data and ensuring regulatory compliance across all regions where the company operates.

6. Security & Data Protection incidents

Security incidents must be managed in accordance with the Security Incident Management Directive, which specifies the response to incidents impacting the confidentiality, integrity, or availability of FLUIDRA's systems. As stated in the Security Incident Management Directive, for incidents involving personal data, coordination with the data protection team is essential to ensure compliance with the applicable regulation.

7. Data Privacy communication channels

The following regional channels are available to address any questions or concerns regarding to this Policy or to data protection matters in general:

- **Europe** (and for the rest of the countries not listed below): dataprivacy@fluidra.com
- **USA:** contact.privacy@fluidra.com
- **Australia:** apacprivacy@fluidra.com

FLUIDRA will endeavour to handle data subject requests on a global, harmonised basis across all regions.

It is mandatory to immediately report any risk of non-compliance or infringement related to personal data.

8. Updates and improvements

This Policy will be reviewed annually and updated when necessary to reflect changes in law or internal practices.

9. Approval, review and supervision

This Policy came into force on **May 4th, 2026** by approval of the **Fluidra Group Board of Directors.**

The Global Internal Audit & Compliance Department shall supervise the extension of this Policy to the subsidiaries and entities of the Fluidra Group that are part of its scope of application. The Global Internal Audit & Compliance Department, as the responsible for this Policy, shall periodically supervise its application.

At least once a year, or upon the occurrence of any event that requires a change in this Policy, the Global Internal Audit & Compliance Department, as the responsible for it, shall proceed to carry out the review, approval, and extension processes to the subsidiaries, as applicable.

10. Review history

Version	Date	Control changes description	Sponsor
1.0	May 4th, 2026	Approval of version 1.0	Global Internal Audit & Compliance Department

FLUIDRA