CANAL+

GLOBAL DATA PROTECTION POLICY

DOCUMENT STATUS					
Version	V1	**Date**	September 2025	**Number of pages**	14

SUMMARY

1 DEFINITIONS - GLOSSARY

"Applicable data protection law" means all data protection or related laws, regulations, guidelines and recommendations of Supervisory authorities, including but not limited to GDPR, applicable to Canal+ Entities.

"Business owner" means any employee of a Canal+ entity initiating a project or a contract involving Personal Data processing activities carried out by one or several Canal+ entity(ies) and who is accountable for ensuring compliance with, and implementing, the recommendations of the Global data protection officer, Local data protection officers and Data protection referents.

"Canal+ Holding" means Canal+ holding acting as the corporate-level parent company of Canal+ Group, responsible for defining Canal+ Group's overall strategic direction and governance, and which directly or indirectly controls the Canal+ Entities.

"Canal+ Entity" or "Canal+ Entities" means any individual company or companies that are part of Canal+ Group, including Canal+ Holding and, without limitation, any subsidiaries, affiliates, or operating entities, directly or indirectly controlled by Canal+ Holding.

"Canal+ Group" means the group composed of Canal+ Holding and all legal entities that are, directly or indirectly, controlled by Canal+ Holding, considered collectively as a single economic and organizational group.

"CISO" means the Chief Information Security Officer.

"Controller", "Consent", "Data Breach", "Data subject", "Personal data", "Processing", "Processor", "Supervisory Authority" shall be interpreted in accordance with Applicable data protection law.

"DPIA" means, when a PIA indicates that a Processing of Personal Data is likely to result in a high risk to the rights and freedoms of natural personal, the Data Protection Impact Assessment conducted by the Controller to determine the nature of those risks and the mitigation measures envisaged to address the risks.

"Data protection referent" means, in countries where the Applicable data protection law does not require the appointment of a data protection officer with a Supervisory Authority, the employee of a Canal+ entity who reports functionally to the Global data protection officer and who is responsible for monitoring and advising on data protection compliance in one specific or several jurisdictions or for one specific or several Canal+ entities.

"EEA" means the European Economic Area.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection).

"Global data protection policy" means this global data protection policy, also referred as "this policy"

"Global data protection officer" means the natural person appointed with a Supervisory Authority and who is responsible for monitoring and advising on data protection compliance across Canal+ Group.

"KPI" means *Key Performance Indicators* and refers to the metric used to measure the effectiveness of data protection compliance across one or more Canal+ entities.

"Local data protection officer" means the natural or legal person internally or externally appointed with a Supervisory Authority who reports functionally to the Global data protection officer and who is responsible for monitoring and advising on data protection compliance in one specific or several Canal+ entities.

"PIA" means the Privacy Impact Assessment conducted by the Controller to determine whether a Processing of Personal data is likely to result in a high risk.

"Privacy by default" means the principle according to which, by default, only the personal data that is necessary for each specific purpose of processing is collected and processed. In particular, systems and tools must be configured in such a way that unnecessary data is not collected, and data can be easily deleted, anonymized, or archived once the retention period has expired.

"Privacy by design" means the set of data protection principles and safeguards that are proactively embedded into the design and development of processed, products, services and IT systems that involve personal data, from the earliest stages and throughout their lifecycle.

"ROPA" means the Record of Processing Activities which is a document created and updated by the Controller with inventory and description of Personal Data Processing activities performed by each Canal+ entity.

"Security Insurance Plan" means the document owned by the CISO and aiming to formalizing and documenting the guarantees expected by a Canal+ entity from a Third party regarding the implementation of technical and organizational security measures.

"Third country" means (1) for a data exporter subject to GDPR or equivalent European data protection law, any country located outside the EEA, (2) for a data exporter not subject to the GDPR or equivalent European data protection law, any country where the Personal data are transferred and which is not the country where the Personal data were originally collected and/or processed.

"Third party" means any natural or legal person with whom a Canal+ entity has existing or planned contractual relations.

"Transfer" means any disclosure, transmission, or making available of Personal data by a Controller to a Third party, including transfers across national borders.

2 PREAMBLE

2.1 *Purpose of the Global data protection policy*

In the context of its activities, Canal+ Group needs to collect and process certain categories of Personal Data relating to its employees, prospects, customers, visitors or any other categories of Data Subjects for different purposes.

Canal+ Group considers the security and protection of individuals' personal data to be a top priority and is committed to implementing high standards, principles and rules of data protection to ensure compliance with Applicable data protection law across all Canal+ entities.

In this context, the Canal+ Group has developed this Global Data Protection Policy to establish a unified data protection framework.

This policy:

- Sets out the Canal+ Group's data protection commitments, applicable to each Canal+ entity
- Provides an overview of the Group's data protection governance structure.

2.2 *Scope of the Global data protection policy*

This policy establishes a common data protection framework and applies globally to all Canal+ entities, regardless of their location. This policy applies to all Processing of Personal data carried out by Canal+ entities, whether acting as a Controller or a Processor.

Since Applicable data protection laws may vary by jurisdiction, each Canal+ entity is responsible for implementing this policy and supplementing it where necessary to ensure compliance with local data protection requirements.

In the event of any conflict or inconsistency between a provision of this policy and a provision related to the same subject matter provided by local data protection requirements, the order of precedence shall be (1) the Applicable data protection laws, (2) the Global data protection policy.

3 DATA PROTECTION COMMITMENTS OF CANAL+ GROUP

3.1 *Key principles for Personal data Processing activities*

3.1.1 *Lawfulness, fairness and transparency*

Canal+ Group is committed to processing Personal data lawfully, fairly, and transparently.

This means that any Processing of personal data by a Canal+ entity can only occur if there is a valid legal basis for it. The conditions under which Personal data Processing is lawful may vary depending on the Applicable data protection regulations.

Where the GDPR applies, Canal+ entities process Personal data only if at least one of the following conditions is met, being understood that GDPR requirements can be supplemented by national data protection laws:

- The data subject has given its consent to the Processing of its Personal data
- Processing is necessary for the performance of a contract to which the Data subject is a party
- Processing is necessary to comply with a legal obligation to which the Canal+ entity is subject
- Processing is necessary to protect the vital interests of the Data subject or another natural person
- Processing is necessary for the performance of a task carried out in public interest
- Processing is necessary for the legitimate interests pursued by the Canal+ entity or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data.

Where other national or regional data protection laws apply, each Canal+ entity ensures that the Processing of Personal data is lawful according to the relevant legal framework.

Furthermore, Personal data collected, stored, or otherwise processed by Canal+ Group is handled fairly and transparently. This means that personal data is processed only for the purposes stated at the time of collection and not in ways that Data subjects would not reasonably expect. Transparency is essential for fair Processing, and each Canal+ entity is committed to informing Data subjects about how their Personal data is processed, in accordance with Applicable data protection laws.

3.1.2 *Purpose limitation*

Canal+ Group undertakes to collect and process Personal data for specific, explicit and legitimate purposes, and to not further process Personal data in a manner that is incompatible with purposes for which Personal data was initially collected.

Canal+ entities will not re-use Personal data for purposes other than those originally intended, except by following the conditions provided by the Applicable data protection law for such re-use of Personal data.

3.1.3 *Data minimization*

Canal+ Group is committed to ensuring that Personal data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected and processed.

Each Canal+ entity shall evaluate the need for collecting Personal data in relation to the specific purpose pursued and refrain from collecting data that is not strictly necessary.

3.1.4 *Limited retention*

Canal+ Group is committed to retaining Personal data only for as long as necessary to fulfill the purposes for which it was collected.

Each Canal+ entity determines appropriate data retention periods through a documented and structured approach, which includes, but is not limited to, the following steps:

- Analyzing applicable laws that may specify data retention periods for certain categories of Personal data or purposes (*e.g., employment law, tax law, accounting law etc.*)
- Considering guidelines and recommendations from Supervisory authorities that define or recommend data retention periods in certain areas
- Where no legal provisions or guidelines exist, conducting an assessment in collaboration with Business owners to define a reasonable data retention period based on the intended purpose(s).

As good practice, each Canal+ entity should document the applicable data retention periods in a data retention repository.

Once the applicable retention period has expired, each Canal+ entity is responsible for deleting, anonymizing, or archiving the Personal data in accordance with Applicable data protection laws and any other legal obligations to which it is subject.

3.1.5 *Security*

Information security is a key element of data protection compliance and Canal+ Group is committed to processing Personal data in a manner that ensures security of Personal data, including protection against unauthorized or unlawful Processing and against accidental loss and destruction.

Each Canal+ entity undertakes to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

These measures are defined and governed by the General Information System Security Policy (GISSP), which sets the organizational principles for managing the security of the information systems within the companies and subsidiaries of the Canal+ Group.

3.1.6 *Privacy by design and by default*

In line with the principles of Privacy by design and Privacy by default, all Canal+ entities commit to ensure that personal data protection is integrated into the specifications, architecture, and operations of business models, processes and IT systems from the earliest stage, during the conceptualization and technical design phases.

Activities, processes, and systems involving Personal data are designed and implemented in a way that ensures compliance with data protection principles and embeds appropriate safeguards by default.

When planning a new project, product, or service that involves processing of Personal data, the Business owner undertakes to consider data protection requirements into account from the very beginning and contact the Global data protection officer, the Local data protection officer, or the Data protection referent, depending on the territorial scope of the personal data processing.

3.2 *Rights of the Data subjects*

Canal+ Group undertakes to duly consider and respect all rights granted to Data subjects under the Applicable data protections laws, and to implement all necessary processes to ensure that any request submitted by a Data subject is handled and fulfilled within the timeframes prescribed by such laws.

Where the GDPR applies, Data subjects may, subject to the limitations and conditions set forth therein, exercise the following rights:

- The right of access
- The right to rectification
- The right to erasure ("right to be forgotten")
- The right to restriction of processing
- The right to data portability
- The right to object
- The right to withdraw the consent
- The right not to be subject to a decision based solely on automated processing, including profiling

Each Canal+ entity that is subject to the GDPR and acts as a Data controller is accountable for upholding these rights and for providing responses to requests from Data subjects in accordance with the requirements of the GDPR. Such responses are provided without undue delay, and, in any event, no later than thirty (30) days from the receipt of the request.

Where other national or regional data protection laws are applicable, each Canal+ entity ensures that the rights of Data subjects are recognized, processed and fulfilled in compliance with the relevant Applicable data protection laws.

In certain circumstances, specific procedures may be implemented by one or more Canal+ entities for managing the exercise of rights by Data subjects. These procedures may define the steps to be followed when a request is made, including the assessment of eligibility of the request and identification of internal stakeholders to be contacted. In such cases, reference should be made to these procedures.

3.3 *Management of Third parties*

Canal+ Group is committed to conducting its business relationships and engaging Third parties in full compliance with Applicable data protection laws.

Third parties may only be engaged if they can clearly demonstrate that they uphold adequate standards and provide appropriate safeguards with respect to the security and protection of Personal Data.

Accordingly, suitable due diligence must be carried out to assess each Third party before entrusting them with any processing of Personal data. This due diligence may encompass various relevant control points, including requirements set forth by Applicable data protection laws, such as the integration of Privacy by Design and by Default principles, the location of the Third party, and the security measures they have implemented.

To support this objective, Business owner, assisted by the Group data protection officer, the Local data protection officer, or the Data protection referent, may rely on the "Privacy Screening" document developed by Canal+ Holding, which contains structured questions across multiple assessment streams.

Furthermore, during the contractual negotiation phase, each Canal+ entity undertakes to incorporate the appropriate contractual clauses with the Third party, in line with Applicable data protection laws. For example, where a Canal+ entity is subject to the GDPR and acts as a Data controller, the agreement concluded with the Third party shall include, at a minimum, the provisions set out in Article 28.3 of the GDPR.

3.4 *International Transfers of Personal data*

Applicable data protection laws may require Canal+ entities to take specific measures to protect Personal data before transferring it out of the country where it was collected. In the case of a Transfer of Personal data, each Canal+ entity is committed to carrying out such Transfer only in accordance with the conditions laid down by the Applicable data protection laws, whether the Transfer is from the EEA or from a country outside the EEA.

3.4.1 *Transfers of Personal data from the EEA to a Third country*

If a Transfer of Personal data from the EEA to a Third country is planned, the Canal+ entity acting as data exporter undertakes to ensure that only Personal data strictly necessary for the intended purpose are transferred, in line with the data minimization principle, and that the Transfer is duly authorized. Such a Transfer may take place only if:

- Personal data are transferred to a Third country for which the European Commission has formally recognized, through an adequacy decision, that the country provides an adequate level of data protection; or
- Appropriate safeguards have been implemented, such as binding corporate rules or standard contractual clauses.

Even if appropriate safeguards have been put in place, each Canal+ entity which transfer Personal data undertakes to assess the legislation and/or practices in force of the Third country that may impinge on the effectiveness of the appropriate safeguards to frame the Transfer and require implementation of supplementary measures. To conduct this assessment, the Transfer Impact Assessment, the Canal+ entity refers to the *Recommendations* 01/2020 *on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*

3.4.2 *Transfers of Personal data from a country located outside the EEA to a Third country*

Certain data protection regulations outside the EEA govern, restrict or prohibit the Transfer of Personal data outside the country in which the data were collected.

Where a Canal+ entity intends to transfer Personal data from a country located outside the EEA to a Third country, it undertakes to perform the necessary due diligence and to take all required steps to ensure that only authorized Transfers are carried out, in compliance with the Applicable data protection laws.

3.5 *Incidents and Data Breach management*

Canal+ Group undertakes to implement the necessary measures to prevent, detect, manage and report security incidents, including Personal data breaches. In this regard, Canal+ Group ensures that appropriate

technical and organizational security measures are in place to protect Personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

Each Canal+ entity is committed to handling identified Personal data breaches in compliance with the Applicable data protection laws and in accordance with the global data breach management policy of Canal+ Group. This includes promptly assessing the breach, taking corrective measures to mitigate any adverse effects, and, where required, notifying the competent Supervisory Authorities and affected Data subjects within the timeframes set by the Applicable data protection laws.

3.6 *Accountability*

Canal+ Group undertakes to implement all necessary measures to ensure, and to be able to demonstrate at any time, that the Processing of Personal data is carried out in compliance with the Applicable data protection laws. Accordingly, each Canal+ entity maintains comprehensive documentation evidencing such compliance, y putting in place measures including, but not limited to, the following:

- Maintaining accurate and up-to-date records of all Personal data processing activities.
- Documenting PIA, DPIA, and Transfer Impact Assessments, as required.
- Performing thorough due diligence prior to engaging any Third party or initiating any new project involving the processing of Personal data, such as by issuing questionnaires to Third parties and conducting Privacy screenings.
- Keeping detailed records of Data subjects' requests that have been fulfilled, as well as of any Personal data Breaches that have been notified.
- Implementing any data protection policies, including this policy, and other internal procedures designed to govern the use of Personal data and ensure compliance with all Applicable data protection laws.

Furthermore, each Canal+ entity undertakes to conduct regular reviews and assessments, in accordance with Article 4.3 of this policy, to monitor and ensure continued compliance with the Applicable data protection laws.

4 GOVERNANCE AND MONITORING OF DATA PROTECTION COMPLIANCE WITHIN CANAL+ GROUP

4.1 *Data protection stakeholders within Canal+ Group*

Canal+ Group has designed and implemented a governance framework across the organization to ensure compliance with Applicable data protection law. This framework defines various roles and responsibilities as outlined below.

Key roles in Data protection.

- **Global data protection officer**

The Global data protection officer is responsible for overseeing and advising on data protection compliance across the Canal+ Group. Their main responsibilities include:

- Informing and advising Business owners and employees involved in data processing about their obligations under the GDPR
- Monitoring compliance with the GDPR, including assigning responsibilities, raising awareness, training staff involved in personal data processing operations, and conducting related audits
- Providing advice, when requested, on DPIA and monitoring their execution
- Cooperating with the Supervisory authorities
- Acting as the primary contact point for the Supervisory authorities regarding personal data processing activities

The Global data protection officer's responsibilities are limited to the scope defined by appointments with the Supervisory authority, which currently include Canal+ Holding, Canal+ France (including overseas territories) and Canal+ Tech. For other Canal+ entities, Local data protection officers and Data protection referents are responsible for ensuring compliance with Applicable data protection laws.

In addition to the tasks explicitly outlined in Article 39 of the GDPR, the Global data protection officer also leads cross-entity data protection initiatives across the Canal+ Group. This includes:

- Promoting a culture of data protection within Canal+ Group
- Organizing and leading data protection committees
- Developing and distributing monitoring tools (e.g., policies, procedures, templates…) to support and document compliance with Applicable data protection law
- Collecting compliance indicators (e.g., KPIs) across Canal+ Group, particularly for internal audits and the annual risk register review required by the UK Corporate Governance Code.

- **Local data protection officers and Data protection referents**

Canal+ Group has established additional roles with formal responsibilities for ensuring compliance with Applicable data protection law within their respective areas.

Local data protection officers are appointed internally or externally and registered with a Supervisory authority. They are responsible for overseeing data protection compliance for one or more Canal+ entities.

Data protection referents are employees of a Canal+ entity responsible for monitoring and advising on data protection compliance within specific jurisdictions or entities.

Their responsibilities include:

- Informing and advising Business owners and employees on their obligations under Applicable data protection law
- Monitoring compliance, including assigning responsibilities, raising awareness, training staff, and conducting audits
- Providing advice on DPIA and monitoring their implementation, where required by law
- Cooperating with the Supervisory authority and acting as a contact point, where required

Additionally, they are expected to:

- Participate in data protection committees
- Share updates on regulatory changes that may significantly impact specific Canal+ entities or jurisdictions
- Implement and adapt monitoring tools provided by the Group data protection officer
- Submit, at least annually, KPI to the Group data protection officer
- Collaborate with the Group data protection officer especially during audits or inspections.

Other key stakeholders.

- **CISO team**

To effectively address security challenges, Canal+ Group has established a dedicated Information System Security organization. This structure is centered around a Security Director and a Chief Information Security Officer (CISO).

The Security Director is responsible for strategic security decisions, the validation of the GISSP, the management of major information security risks, and for seeking support of arbitration from the Group CTO during Steering Committees where critical security matters are discussed.

The CISO oversees the operational implementation of the GISSP. He ensures that each department carries out actions to assess deviations and ensure compliance with the GISSP. To do so, the CISO relies on technical ambassadors embedded within the various business units to deploy controls across the entire organization.

This organizational framework is detailed in the GISSP.

- **Business owners**

Business owners are employees who initiate projects or contracts involving Personal data processing withing one or more Canal+ entities. They are accountable for ensuring compliance with, and implementing, the recommendations of the Global data protection officer, Local data protection officers and Data protection referents.

4.2 *Data protection committees*

The Data Protection Committees bring together the Global data protection officer, Local data protection officers, and Data protection referents.

Its objectives are as follows:

- Discuss the latest regulatory developments and news impacting data protection
- Present and share monitoring and control tools developed by the Group data protection officer
- Collect feedback from Local data protection officers and Data protection referents, particularly regarding the deployment and/or adaptation of tools within the relevant Canal+ entities
- Optimize the management and oversight of intragroup projects involving personal data.

The Data protection Committee meets at least quarterly.

4.3 *Data protection compliance monitoring*

Canal+ Group is committed to implementing appropriate and effective tools to ensure and document compliance with applicable data protection laws.

To this end, each Canal+ entity may rely on documentation provided by the Global data protection officer, including templates (e.g., data processing agreements, PIAs, DPIAs, KPIs), policies and procedures.

However, Local data protection officers and Data protection referents are responsible for deploying and adapting these documents to meet the specific requirements of Applicable data protection laws. They are also expected to develop and implement additional tools when necessary to ensure and demonstrate compliance.

Furthermore, each Canal+ entity undertakes to conduct periodic reviews to assess its level of compliance. The scope of these assessments may be based on:

- Previous audits and reviews,
- Regulatory updates or developments,
- Discussions with Supervisory Authorities,
- Regularly collected KPIs.

These assessments aim to identify residual compliance gaps, evaluate risk appetite and define action plans with appropriate remediation measures.

In addition to assessments conducted by the Global data protection officer, Local data protection officers, or Data protection referents, any Canal+ entity may be subject to internal audits on data protection matters, in accordance with the Canal+ Group internal audit program.

5 AMENDMENTS TO THE POLICY

Canal+ Group will periodically review this policy to evaluate its continued relevance and consistence, ensure adherence to evolving regulatory requirements, and reinforce a culture of data protection within the group.

These reviews will also serve to monitor the effectiveness of implemented measures, identify areas for enhancement, and drive continual improvement across all data processing activities.

Through this ongoing commitment, Canal+ Group seeks to uphold the highest standards of personal data protection and to foster trust with all stakeholders, including customers, employees, and partners.