ITV Group Data Protection & Privacy Policy

Status: Final
Document Type: Policy

Contents

1. Introduction

ITV is committed to working with data in a compliant manner, ensuring quality, consistency, usefulness, and safety, and protecting our users' privacy.

Protecting ***Personal Data*** is a responsibility shared by all ITV employees, freelancers and contractors. Any failure to handle ***Personal Data*** properly will be a breach of the law and may result in both significant financial and reputational loss to ITV. ITV could face fines of up to 4% of annual turnover and legal action.

This Policy sets out how ITV collects, stores, analyses, uses or otherwise processes or handles ***Personal Data***. This Policy is supplemented by, and should be read alongside, other data protection and privacy standards, procedures and guidance that may be specific to your jurisdiction or business area (including those listed at the end of this Policy).

The use of jargon is limited - but you can refer to the *Key Terms* below.

2. What is Personal Data

Personal data (also referred to as personal information) is broadly defined. It includes any information that makes a person identifiable. This can be either direct or indirect, for example by reference to:

- an identifier such as name, identification number, location data, online identifier (e.g. IP address, ITV ID, and various types of cookies such as those used for tracking online activities, saving user preferences, and collecting information on online behaviour); or
- anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Data, including 'special categories of data', requires higher levels of protection and specific handling in many jurisdictions. This includes information concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- information concerning health, sex life or sexual orientation;
- genetic/biometric data obtained to identify a person; and
- criminal convictions and offences.

We must take particular care in the processing of this sensitive personal data as the law requires us to take further steps to safeguard it.There are strict conditions around processing the special categories of personal data and that relating to criminal convictions and offences. Please read and follow ITV's *Policy for Processing Special Category & Criminal Offence Data*.

3. Principles

As part of our business activities, ITV processes large amounts of ***Personal Data***. As a starting point, our approach to handling ***Personal Data*** should reflect the following high level principles:

- **Enabling**: enable ITV to derive value from the personal information it processes, to help us become More than TV;
- **Protective**: protect the information rights of our viewers, people, customers, contractors, talent, contributors and colleagues; and
- **Ethical**: ensure that ITV is transparent, responsible and accountable in its processing of personal information, to maintain trust in the ITV brand, and ensure the sustainability of ITV's data strategy.

ITV seeks to protect and responsibly handle all ***Personal Data*** by complying with applicable laws and regulations. This means that all ***Personal Data*** must be:

- collected and processed in a lawful, fair and transparent manner;
- collected for a specified, explicit and legitimate purpose or purposes;
- adequate, relevant and limited to what is necessary for the purposes of the processing;
- accurate and, where necessary, kept up to date;
- kept no longer than is necessary to fulfill the specified purpose; and
- kept secure by using appropriate technical and organisational measures.

ITV is accountable for upholding these principles and is responsible for demonstrating its compliance with these principles. To help you, we have described what you need to do:

Principle	Requires that we..
Lawfulness, transparency and fairness	Only collect, use, share and store ***Personal Data*** where there is a reasonable need to do so and **transparently** tell individuals how their personal data will be used.
Purpose limitation	Only collect ***Personal Data*** for specific, explicit, legitimate purposes and shouldn't be processed in a manner incompatible with those purposes. We must notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.
Data Minimisation	Ensure ***Personal Data*** is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed. Only collect and use ***Personal Data*** to the extent that it is required for the specific purpose notified to the data subject or in ways that the data subjects might reasonably expect ITV to use their personal data.
Accuracy	Make sure that ***Personal Data*** held is accurate and kept up to date

	and all reasonable steps are taken to destroy or amend inaccurate or out-of-date data.
Storage Limitation	**Keep *Personal Data* in a format which enables the identification of individuals for no longer than necessary to achieve the purpose. *Personal Data*** should be kept for no longer than is necessary for the purpose or purposes for which they were collected. And all reasonable steps taken to destroy, or erase from our systems, all data which is no longer required. See also ITV's Retention Policy.
Security, Integrity & Confidentiality	Store ***Personal Data*** in a secure and confidential way. Engage and work with the CyberSecurity Team to ensure any processing of ***Personal Data*** by us, or third parties on our behalf, meets our internal security policies and controls. ITV will only process ***Personal Data*** we hold in accordance with our Cyber Security and other data security policies which ensures that we take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, ***Personal Data***.
Accountability	Comply with ITV Policies and related procedures and guidelines and continuously assess risk, implement appropriate policies and procedures and keep them under review to ensure they remain effective.

4. Scope & Compliance

A. What this Policy applies to

Within the United Kingdom and the European Economic Area (EEA), the General Data Protection Regulation (UK and EU GDPR) will apply to the processing of personal information (the Data Protection Act 2018 also applies in the UK). Separate laws will apply in other countries that we operate in. Each ITV business is responsible for ensuring compliance with local data protection legislation or regulation to the extent it is broader or more onerous than GDPR. For advice on laws outside of the EEA and the UK, please refer to ITV's Data Protection & Privacy Team.

B. Who this Policy applies to

The scope of this Policy applies to ITV Group including all divisions, labels, subsidiaries, departments, sites, and operations globally and to all ITV colleagues (staff, contractors and freelancers working for ITV). ITV Group includes all companies which are controlled, or more than 50% owned, by the ITV group). Any areas that maintain their own policies, procedures and risk registers must ensure their policies, procedures and practices are aligned to this Policy and related procedures.

Failure to comply with this Policy may subject ITV to civil and/or criminal liability and may result in disciplinary action, including dismissal.

5. Exceptions

If there is a situation where you, or you know ITV cannot comply with this Policy, or you need to apply an exception (for example, where there is a local conflict of law), please contact your Legal & Business Affairs representative or ITV's Data Protection & Privacy Legal Team for guidance.

All decisions to apply an exception to this Policy, including the reasoning behind the decision, must be recorded and filed by the ITV Data Protection & Privacy Legal Team, subject to ITV's Data Governance Framework.

6. Data Governance Framework

ITV has put in place a Data Governance Framework to identify and manage risks and opportunities with respect to the collection and use of data, including ***Personal Data***. Data Owners for each of the ITV business areas in scope for compliance with this Policy, are responsible for the processing activities in their respective parts of the business. Data Owners must therefore ensure compliance with this policy and law, and manage privacy-related risks and issues in their areas. This includes ensuring Data Protection Impact Assessments (DPIAs) are completed and mitigating actions implemented where required.

Data Owners should identify any significant data protection and privacy risks that have an effect across their business and should consult ITV's Global Data Protection Officer and/or the Data Protection & Privacy Legal Team if necessary.

ITV's Global Data Protection Officer and/or the Data Protection & Privacy Legal Team will advise the business and the Data Owners on compliance with applicable laws and regulation.

The Global Data Protection Officer, with the support of the DP Office, will monitor compliance with applicable law, report to senior management on compliance, raise awareness of privacy matters, cooperate with data protection authorities (DPAs), and act as a contact point for individuals regarding the processing of their ***Personal Data***.

The roles and responsibilities of ITV employees responsible for handling ***Personal Data*** in accordance with this Policy are described in more detail in the *ITV Data Ownership Policy* and in the *ITV Data Governance Framework* documents (which sets out the governance operating model).

7. Training

ITV will provide annual, mandatory Data Protection & Privacy training to all ITV employees. Such training will be reviewed on an annual basis. Specific training for particular roles will also be provided where relevant.

8. Collecting & Processing Personal Data

When collecting ***Personal Data***, we should ensure that there is a lawful basis and each individual is provided with transparent information about the processing of their data (this is usually done using a privacy notice). All privacy notices should explain the nature and purpose of the processing and information about privacy rights, using clear and plain language.

We must only process personal information if it is lawful to do so.

Where the lawful processing is based on consent from the individual, this must be freely given, unambiguous, separate from other matters (for example, not bundled into the terms of use), in an intelligible and easily accessible form, using clear and plain language. It should be as easy to withdraw consent as to give it.

Care must be taken when collecting and processing children's data as parental consent may be required. In the UK the ICO Age Appropriate Design Code must also be adhered to. Please seek the advice of Data Protection & Privacy Legal where this applies.

9. ITV Record of Processing Activities (ROPA)

Organisations like ITV are required by law to maintain a Record of Processing Activities for data protection, privacy, security and retention governance and accountability purposes. More details are set out in the ITV Group Procedure for keeping records of processing activities (ROPA).

Each business area is responsible for providing information about its ***Personal Data*** collection and processing activities needed to maintain the ROPA as an up-to-date inventory of all the personal data processing activities. Updated records must also be provided when new processing activities commence or significantly change. All entries on the ROPA must be reviewed by each responsible business area on at least an annual basis.

ITV's ROPA will be kept and maintained by the ITV DP Office.

While records containing ***Personal Data*** are retained in accordance with our *Retention Policy*, we must all regularly review and delete ***Personal Data*** which is no longer required. See ITV's *Retention Policy* and related procedures and guidelines for determining retention periods.

10. Privacy by Design and Default

When a new product, service or production, which involves the processing of ***Personal Data*** (for example a programme-related app, a new service or feature, or the adoption of a new system or tool), is planned or designed, appropriate measures must be implemented to safeguard personal data and to adhere the principles in this Policy.

There must be by default, technical and organisational measures implemented to process ***Personal Data*** to comply with the data protection principles and protect the rights and freedoms of data subjects. Privacy by design and default will also be important when a significant change is made to an existing process or system.

Such measures could include building in privacy controls to user interfaces, applying privacy-enhancing techniques such as pseudonymisation, and regularly reviewing privacy risks. Such measures must be **considered at the design stage** of any new initiative.

11. Risk Assessment

Where processing of ***Personal Data*** is likely to result in high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) must be completed prior to commencement of the processing. To determine if a DPIA is required, you may be asked to complete a ***Threshold Assessment***.

Where one or more risk factors apply, it is likely that a DPIA will be required. Examples of risk factors include, but are not limited to, the following:

• Data processed on a large scale, taking into account the number of individuals concerned, the range of information being processed and the geographical extent of the processing activity • Evaluation or scoring, for example for building marketing or behavioural profiles • Decisions based on automated processing, or example automated CV or applicant screening • Activities involving vulnerable individuals • Sensitive information, including special categories of data • Risk of harm if there is an unauthorised	• Biometric/genetic (e.g. gene/parental test results, fingerprints, retina scans) • Tracking individuals' behaviour • Systematic monitoring to observe or control individuals, for example where CCTV or site access controls are used • Covert filming/audio, for example for investigative journalism purposes • New technology not used before which processes personal information • Data sets that are matched or combined to produce insights regarding individuals

disclosure of information • Information related to criminal offences or convictions	• Personal information is transferred to another country • Information collection without the individual's knowledge

It may not be possible to complete a DPIA prior to commencement of the processing in all circumstances, and exemptions may apply. The DPIA must include details of the measures that will be applied to mitigate the identified privacy risks.

In exceptional circumstances, the relevant DPA may need to be consulted on a processing activity. If the DPA specifies the adoption of risk mitigation measures, these must be in place before the processing may commence.

The Data Protection & Privacy Team will guide you through completion of the DPIA - see also *Data Processing Impact Assessment Procedure and related guidelines.*

12. Individuals' Rights and Requests

In addition to the information that must be provided to individuals before processing their ***Personal Data***, data subjects have other rights, such as:

- Right of access (also called a 'Data Subject Access Request' / DSAR)
- Right to rectification
- Right to request erasure (also known as 'right to be forgotten')
- Right to restriction of processing
- Right to be notified and informed
- Right to data portability
- Right to object to processing (including for direct marketing purposes)
- Right against automated decision making (including profiling)
- Right to complain to the relevant supervisory authority (e.g. the Information Commissioner's Office in the UK).

ITV must comply with rights requests without undue delay and, where applicable, in accordance with time limits set out in law. Where a rights request has been received, this must be forwarded to the Data Protection & Privacy Legal Team by emailing privacy@itv.com .

The Data Protection & Privacy Legal Team will have oversight of, and coordinate responses to, all individuals' rights and requests. Data Owners are responsible for executing rights requests, for example deleting information in response to a right to erasure request or providing information.

ITV is committed to responding to complaints in a timely manner, and without prejudice to the individual making the complaint.

For further details please read and follow *ITV Data Subject Access Requests Procedure*.

13. Third Parties & Data Sharing

ITV's activities often require the sharing of data with, or use of data obtained from, third party individuals or companies. Where this is the case, ITV must carry out appropriate due diligence in relation to the arrangement, in particular regarding data protection and privacy risks. For further information, see separate *ITV Third Party Security Policy* or consult your Legal & Business Affairs contact or the Data Protection & Privacy Legal Team.

When transferring personal data to, or outsourcing processing activities to a third party, please make sure that:

- the third party will handle the data in compliance with the relevant legislation and regulations,
- the processing is governed by a contract or legal data processing agreement.

In addition, the *ITV Third Party Security Policy* which must be followed includes the third party completing the ITV CyberSecurity assessment via Prevalent (the CyberSecurity Team's assessment tool). Please complete the Supplier Onboarding Form to commence this process or contact cybersecurity@itv.com for guidance.

In the case of data sharing personal data within ITV internally, it should be based on existing policies and procedures. If an internal request for date data falls outside of standard practice or agreed purpose for the data, or ad hoc in nature, this must be assessed to ensure the sharing is lawful. For further information, Consult your Legal & Business Affairs contact or the Data Protection & Privacy Legal Team.

14. International Data Transfers

Not all countries provide the same level of protection as GDPR gives to individuals' data. Therefore, before any personal data is transferred internationally please work with your Legal & Business Affairs contact to carry out a ***Transfer Risk Assessment*** and ensure that adequate safeguards are in place, which include enforceable and effective data subject rights.

Where any international data transfer is undertaken via a third party processor, an appropriate contract must be put in place to provide adequate safeguards, before any transfer takes place.

15. Information Security and Incident Response & Management

Personal data breaches can result in a risk to the rights and freedoms of the individuals, as well as reputational damage for the ITV brand and substantial fines based on our global revenue. We are all

responsible for using our systems and technology (whether they are owned by ITV or provided by a third party) in accordance with *ITV's Cyber Security and other Information Security Policies* and the *ITV Code of Conduct*. Standards and controls for maintaining the security and integrity of **all** sensitive and commercial data is the responsibility of the CyberSecurity Team. For any queries relating to data security, please contact your local Cyber team representative or cybersecurity@itv.com.

You should be vigilant to any cyber or information security threats and use all appropriate security controls to safeguard our systems, and the ***Personal Data*** processed by them. If you become aware of any incident or suspected data breach, you must immediately inform your line manager and Data Protection & Privacy Legal Team privacy@itv.com as well as cybersecurity@itv.com.

The Global Data Protection Officer and Data Protection & Privacy Legal Team will coordinate the response to the incident including, if required, reporting it to the DPA within the appropriate timescale (for example within 72 hours in UK/EU) and establishing whether it is necessary to contact the individuals concerned.

See also *ITV Incident Response Guidelines* which provides more details on the types of incidents which should be reported.

16. Dealing with Regulators & DPAs

ITV will cooperate with Regulators and DPAs and respond to any enquiry or request in a timely manner. Data Owners must notify the Data Protection & Privacy Legal Team privacy@itv.com whenever they receive any communication or requests from a Regulator or DPA.

17. Notifications, Escalation & Approvals

Scenario	Communication		By Whom?
	Prior notification	Prior Approval	
Security Incident or suspected data breach	X		CISO & Global DPO (see section 14)
New processing activities triggering requirement for DPIA	X		Legal & Business Affairs team with support of Data Protection & Privacy Legal Team
High Risk Processing or	X	X	Data Protection & Privacy Legal Team

Automated decision-making (including Profiling)			(see section 10)
Onboarding new suppliers processing personal data	X	X	CyberSecurity Team and Legal & Business Affairs team with support of Data Protection & Privacy Legal Team (see section 13)
Data Subject complaints	X		Data Owners working with Legal & Business Affairs team - escalate to Data Protection & Privacy Legal Team if Individual rights or request (see section 11 and below)
Individual rights and requests	X		Data Protection & Privacy Legal Team via privacy@itv.com - team will manage response to the individual
Regulator Enquiries or enforcement action	X	X	General Counsel & Global DPO (see section 16)
International Data Transfers	X	X	Data Protection & Privacy Legal Team (see section 14)

18. Updating this Policy

This Policy is owned and maintained by the Global Data Protection Officer. Compliance with this policy and relevant laws is monitored by the Global Data Protection Officer and the DP Office.

This Policy will be reviewed annually from its publication date, or sooner if there is a relevant change to the law, regulations or business practices. For more information about any aspect of this Policy, please contact privacy@itv.com.

19. Key Terms used in this Policy

CISO means ITV's Chief Information Security Officer

Data Controller means the natural or legal person (e.g. company), public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Typically this will be an ITV company.

Data Processor means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller. Typically this will be one of ITV's suppliers.

Data Owners are designated employees in ITV that are responsible for ensuring that all data-related policies, including this one, are adhered to in the business areas they operate. Data Owners will be those individuals as determined by *ITV Data Ownership Policy* in accordance with the *ITV Data Governance Framework*.

DPA means a privacy or data protection regulator or authority (for example the UK Information

Commissioner's Office).

DPIA means a Data Protection Impact Assessment designed to assess the necessity and proportionality of prospective new or modified processes, technologies and systems, and to assess the risks to individuals' rights and freedoms resulting from such processing, as well as to determine the measures to address such risks.

DP Office means the data protection and privacy compliance team supporting the work of ITV's Global Data Protection Officer.

Data Subject means any natural person identified or identifiable by his/her personal data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Global Data Protection Officer or Global DPO means the designated Data Protection Officer for ITV, who will assist in monitoring internal compliance, inform and advise ITV on its data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for individuals and data protection authorities.

ICO or Information Commissioner's Office means the UK data protection regulator.

Personal Data, also referred to a personal information, means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Process or Processing, in relation to personal information, means any operation or set of operations which is performed on the personal data or sets of personal data, whether or not by automatic means, which includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making the personal data available, alignment or combination, restriction, erasure or destruction.

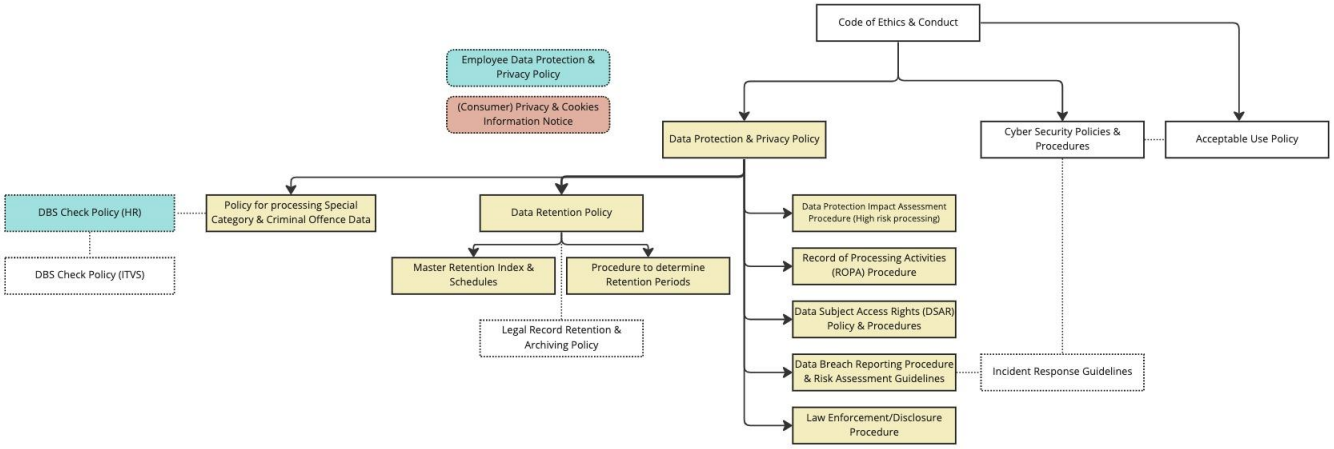
Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

ROPA means the Record of Processing Activities which organisations like ITV are required by law to maintain for data protection, privacy, security and retention governance and accountability purposes.

Sensitive Data means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health, sex life or sexual orientation. In Europe under the GDPR, these are known as Special Categories of Data. For our purposes, information related to criminal convictions and offences should be treated as sensitive data.

See full Key Terms document here.

20. Related Documents



And all other Policies & Procedures published on myITV.

21. Document Control

Date of approval	16 December 2022
Next Review date	1 January 2024
Document replaces	Data Protection & Privacy Policy (published in 2018 and 2019)
Author	Elizabeth Kiernan, Global Data Protection Officer
Reviewed by	Members of the Tech & Data Working Group (during Sep/Oct 2022): Lisa Pashley - Head of Data Protection Compliance Kirsty Benn-Harris, Director of Data Governance Tony Jowett, CISO Chris Williams, Head of Security Risk & Monitoring
Approved by	Kyla Mullins, General Counsel & Corporate Secretary on 12 December 2022 Ratified by Data Oversight Steerco on 16 December 2022

Change record

Version Number	Date	Changes Made	Comments/status
1.0	November 2019	Data Protection & Privacy Policy	Published
2.0	Unknown	New Policy created (Global DPO, Sarah Pozner)	Published
3.0	June 2022	Policy updates - Requirements for identifying and assessing high risk personal data processing and when to work with the Data Protection & Privacy Legal Team to document "Data Protection Impact Assessments" (DPIAs); - Instructions as to when escalation and approvals are necessary; - Removal of reference to DPRS (Data Processing Retention Schedule) - The Data Protection & Privacy Legal Team maintain the statutory Record of Processing Activities (ROPA) on behalf of each ITV business/division; - Link out to new Key Terms (glossary) which will be separately maintained and kept up to date; - Details as to who to contact for more information or to answer questions; - Updated list of Related Documents.	Adopted by Data Privacy Team, awaiting publication on new Data Governance Site on myITV
3.1	Nov 2022	Reformatted to follow the new Group standard format clarifying scope and including links to new/updated policies and procedures including new Procedure for keeping records of processing activities (ROPA).	Approved and Published on 12 December on myITV