



# Personal Data Protection and Privacy Policy

## Approval

### Preparer:

\_\_\_\_\_  
Gary Brown  
Chief Privacy Officer

### Owner:

\_\_\_\_\_  
Electronically Approved\*  
Gary Brown  
Chief Privacy Officer

### Approver:

\_\_\_\_\_  
Electronically Approved\*  
Nathan Harsch  
Vice President & Chief Compliance Officer

\*Electronically approved records are authenticated in the Business Management System (BMS).

*This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its affiliates, subcontractors and/or suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you. Any unauthorized use of this document is prohibited.*



**Table of Contents**

1.0 Policy Statement..... 3

2.0 Key Definitions under the Applicable Data Protection Laws ..... 3

3.0 Principles Governing the Processing of Personal Data ..... 5

4.0 How Westinghouse uses Personal Data ..... 5

5.0 Notifying Data Subjects ..... 6

6.0 Personal Data Sharing..... 6

7.0 Cross-Border Personal Data Transfers ..... 7

8.0 How we Protect Personal Data ..... 7

9.0 Retention of Personal Data..... 7

10.0 Data Subject’s Rights and Requests ..... 8

11.0 Guidelines to Westinghouse Representatives ..... 9

12.0 Revision Summary..... 10



## LEGAL

### Personal Data Protection and Privacy Policy

---

#### 1.0 Policy Statement

Westinghouse is committed to doing business ethically, honestly and in compliance with applicable laws and regulations. This includes compliance with all Applicable Data Protection Laws where Westinghouse does business.

The purpose of this Policy is to set out the principles and legal conditions for Westinghouse to obtain, handle, process, transport or store Personal Data (as defined below), and to outline the rights granted to the individuals to whom the data belong (residents collectively of all jurisdictions, the **"Data Subjects"**) under Applicable Data Protection Laws, and to establish the rules and legal conditions under which Westinghouse's employees, agents and representatives, including our independent contractors, will process Personal Data.

This Policy is applicable to all Westinghouse entities, including Westinghouse Electric Company LLC and Westinghouse Electric UK Holdings LTD., their wholly-owned or controlled subsidiaries and joint ventures, and all organisational units owned, managed, or reporting to them and their senior management anywhere in the world (collectively, **"Westinghouse"**, the **"Company"**, **"we"**, **"us"**, or **"our"**).

During business operations, Westinghouse may collect and process Personal Data of Data Subjects located in the countries where we operate. This may include Personal Data received directly from a person (for example, employees' data) and data received from other sources (including, for example, customers, suppliers, business partners and others). This Policy applies to all Personal Data we collect, maintain, transmit, store, retain or otherwise use, regardless of the storage media used or whether it relates to employees, contractors, customers or any other Data Subject.

The Global Compliance Organisation is responsible for ensuring compliance with all Applicable Data Protection Laws and with this Policy. The Global Compliance Organisation is also responsible for administering and overseeing implementation of this Policy and all the Policies on privacy and data protection and, as applicable, developing related operating guidelines, procedures, processes, policies and notices.

The Global Compliance Organisation will conduct periodic reviews and audits to assess policy compliance. Any breach by Westinghouse Representatives (as defined below) of this Policy and related policies, operating procedures or processes designed to protect Personal Data of Data Subjects located in the countries where we operate may result in disciplinary action, up to and including termination of employment to the extent permitted by law.

#### 2.0 Key Definitions under the Applicable Data Protection Laws

##### 2.1 Data Subject

The individual (e.g., the employees, the contingent laborers, the contact persons of customer or suppliers, interns, volunteers, etc.) about whom Personal Data is collected and stored. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

##### 2.2 Personal Data

Information identifying or relating to a Data Subject that either identifies or can be combined with other data in our possession or readily accessible to identify (directly or indirectly) a Data Subject. Some jurisdictions may call this Personally Identifiable Information (PII). Personal Data includes, but is not

---



## LEGAL

### Personal Data Protection and Privacy Policy

---

limited to, name, email address and phone numbers (including personal and Company e-mail address and phone numbers), date of birth, any identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, economic, cultural or digital identity of the Data Subject. For more information on personal data please see the **Personal Data Identification Policy** (BMS-LGL-151).

#### 2.3 Sensitive Personal Data

Personal Data that, by their nature, are particularly sensitive in relation to fundamental rights and freedoms and therefore merit specific protection. This is sometimes called 'Special Category Data' or "Sensitive Personal Data". Sensitive Personal Data is a category of Personal Data and includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, criminal conviction or offences, biometric, personal images or voice recordings, genetic data, precise geolocation, or contents of a data subject's email/mail/text. Processing Sensitive Personal Data can only occur under strict conditions, such as permission under applicable laws and/or the written consent of the Data Subject.

#### 2.4 Processing

Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

#### 2.5 Data Controller

Person or legal entity that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Applicable Data Protection Laws. In Westinghouse, the Data Controller generally is Westinghouse Electric Company LLC and/or the entity with which, as the case may be, employees have an employment contract or at which employees may be assigned to, or with which contractors or business partners have a contract.

#### 2.6 Processor

Person or legal entity that processes Personal Data on behalf of the Controller.

#### 2.7 Business

Any for-profit legal entity that collects Personal Data on its own or on behalf of others; that alone or jointly with others determines the purposes and means of the processing.

#### 2.8 Service Provider

Any for-profit legal entity that processes or collects Personal Data on behalf of a business and operates under a service provider contract.



## LEGAL

### Personal Data Protection and Privacy Policy

---

#### 2.9 Data Security Incident

Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational protections that we or our third-party service providers put in place to protect it. The loss, unauthorized access, disclosure or acquisition of Personal Data is a Data Security Incident. For further information on data security incidents please see the **Data Security Incident Reporting and Response Policy** (BMS-LGL-108).

#### 2.10 Applicable Data Protection Laws

All laws and regulations governing the protection of individuals with regard to the Processing of Personal Data, including, but not limited to: (a) the General Data Protection Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 (“**GDPR**”) and any national law implementing or supplementing the GDPR; (b) the UK Data Protection Act 2018 or any future UK laws or regulations, (c) the Brazilian General Law on Protection of Personal Data (“**LGPD**”), (d) the China Personal Information Protection Law (“**PIPL**”), and (e) the California Privacy Rights Act (“**CPRA**”).

### 3.0 Principles Governing the Processing of Personal Data

The following are the main principles governing the Processing of Personal Data under the Applicable Data protection Laws, to which Westinghouse adheres when collecting and processing personal data:

- **Lawfulness, Fairness:** Collect and use Personal Data fairly and only for lawful and specified purposes related to our legitimate business objectives where the locally applicable laws allow.
- **Purpose limitation:** Limit the collection of Personal Data to what is adequate, relevant, and not excessive for the intended purpose.
- **Transparency:** Notify individuals about the Personal Data Processing practices in a clear and transparent manner.
- **Accuracy:** Ensure the accuracy of the Personal Data we collect, hold and use (reasonable steps must be taken to ensure that Personal Data are accurate, complete and current).
- **Storage limitation:** Retain Personal Data for the shortest period necessary to fulfil the established purpose and the applicable statutory records retention requirements.
- **Respect Data Subjects' rights:** Establish policies and procedures to enable Data Subjects to exercise their rights and to ensure that any Data Subjects' requests are addressed timely and consistently.
- **Integrity and confidentiality:** Secure the Personal Data we hold.

### 4.0 How Westinghouse uses Personal Data

Westinghouse may only collect and process Personal Data for specified purposes reasonably necessary to accomplish our legitimate business objectives.

As an example, Westinghouse processes a number of Personal Data about its employees and contingent laborers including, but not limited to, personal information such as name, date of birth and

---



## LEGAL

### Personal Data Protection and Privacy Policy

---

other biographical and demographic information, educational background, contact details, job-related information and employment history, salary-related information, government-issued ID numbers and tax ID numbers, such as US Social Security numbers, financial information and banking details, membership in pension plans, online identifiers, data about the use of Company-provided information systems. Westinghouse may also process certain Sensitive Personal Data of the employees.

Westinghouse holds and processes necessary Personal Data about the contact persons at customers and suppliers for the purpose of managing the business relationship with the customers and suppliers.

Westinghouse primarily uses the Personal Data to:

- Conduct day-to-day business;
- Manage contractual relationships;
- Comply with applicable legal and/or regulatory obligations and requirements;
- Manage the relationship with competent public authorities and financial institutions;
- Perform data analytics for the purpose of operating, evaluating, and improving our business;
- Project, assess, negotiate and implement extraordinary corporate transactions (mergers, acquisitions, transfer of business or certain assets, etc.);
- Maintain and enhance the safety and security of network services, information resources, and employees.

The legal basis for Westinghouse processing the Personal Data will typically be one of the following:

- **The performance of a contract with a Data Subject,**
- **Compliance with legal obligations binding on Westinghouse,**
- **Westinghouse legitimate business interests; or,**
- **The Data Subject's specific consent.**

## 5.0 Notifying Data Subjects

Westinghouse shall clearly notify the Data Subjects about how and why we will use, process, disclose, protect and retain Personal Data through a dedicated privacy notice (either generic or specific to certain purposes).

Where required by applicable law, we will request the Data Subjects' consent for the Processing of Personal Data belonging to them in a particular way, and those Data Subjects will be provided with an opportunity to choose if they want their Personal Data used in that way.

## 6.0 Personal Data Sharing

Westinghouse will not disclose or share personal data to third parties for marketing purposes.

Westinghouse is an international group of companies operating around the globe. Thus, Personal Data may be shared among Westinghouse group companies for the purposes described in this Policy or other purposes specified in the privacy notices.

Westinghouse may also share Personal Data with consultants and service providers that are retained for advice and/or to perform services on our behalf (such as accountants, auditors, attorneys or other

---



## LEGAL

### Personal Data Protection and Privacy Policy

---

consultants, to business area associations, banks and to other public or private entities, such as health-related entities, Social Security corporate bodies, public financial offices, payroll service providers and IT service providers). These third parties service providers shall be contractually bound to process Personal Data in compliance with Westinghouse instructions and to safeguard the Personal Data in compliance with Applicable Data Protection Laws and are restricted from using or disclosing Personal Data except as necessary to perform services on our behalf or to comply with legal requirements.

If required or permitted to do so by applicable laws, Westinghouse may disclose the Personal Data to law enforcement authorities, other government officials or other third parties as required by law.

## 7.0 Cross-Border Personal Data Transfers

Given the multinational nature of Westinghouse, Personal Data collected may be stored in countries different from where they were collected or where the data originated.

Applicable Data Protection Laws in certain countries where we operate may restrict these cross-border Personal Data transfers.

Westinghouse will transfer Personal Data only for the purposes described in this Policy or specified in the privacy notices and, in compliance with the Applicable Data Protection Laws, will take all necessary measures to ensure that all cross-border transfers are adequately protected. This includes using appropriate protections such as the EU Standard Contractual Clauses for the transfer of Personal Data to from the EU to third countries, which the European Commission has assessed as providing an adequate level of protection for personal. A copy of such appropriate protections can be obtained by contacting the Global Compliance Organisation as set out below.

## 8.0 How we Protect Personal Data

The security and confidentiality of all Personal Data is of the utmost importance to Westinghouse. Westinghouse maintains administrative, technical, and physical measures to protect Personal Data against unlawful or unauthorized destruction, loss, alteration, use, disclosure, or access in compliance with Applicable Data Protection Laws.

To safeguard the integrity of Personal Data, access to such Personal Data is granted on a need-to-know basis, limited only to those employees who need access to such data in order to carry out the functions of their jobs.

Employees must comply with all applicable aspects of the Westinghouse Information Security Program and Policies, and shall comply with, and will not attempt to circumvent, the administrative, physical, and technical safeguards implemented by the Company in order to maintain and protect Personal Data from the point of collection to the point of destruction.

## 9.0 Retention of Personal Data

Westinghouse retains Personal Data in its systems and archives as per the **Personal Data Record Retention Policy** (BMS-LGL-156). Effectively, this as long as: (1) it is needed for the purposes for which the Personal Data were obtained, in accordance with the provisions of this Policy and legal and contractual requirements, or (2) Westinghouse has another lawful basis, stated in this Policy or at the point of collection, for retaining that information beyond the period for which it is necessary in order to serve the original purposes.



## LEGAL

### Personal Data Protection and Privacy Policy

---

When Personal Data is no longer necessary for the purposes for which it is processed, it is deleted or kept in a form which does not permit the identification of Data Subjects, provided that Westinghouse is not legally required or permitted to hold such Personal Data.

Personal Data shall be made available for the review upon request by Data Subjects. A fee may be charged in case more than one copy of the Personal Data is requested.

## 10.0 Data Subject's Rights and Requests

Data Subjects have rights when it comes to how Westinghouse handles their Personal Data. These rights vary depending on the where the Data Subject resides, but may include:

- **Right of access:** right to obtain from the Data Controller a confirmation as to whether or not your Personal Data is being processed, and, if so, to demand to have access to your Personal Data.
- **Right to rectification:** right to require the Data Controller to correct inaccurate or incomplete Personal Data.
- **Right to erasure (right to be forgotten):** right to obtain the erasure of Personal Data without undue delay, where the request is made in accordance with the Applicable Data Protection Laws.
- **Right to object to data processing:** right to object at any time to the Processing of Personal Data based on the legitimate interest of the Data Controller, on grounds relating to the Data Subject's particular situation.
- **Right to limit the data processing:** right to obtain from the Data Controller a limitation on the processing activities when the accuracy of Personal Data is disputed, and for the time necessary for the Data Controller to verify the accuracy of Personal Data.
- **Right to data portability:** right to receive the Personal Data provided to the Data Controller in a structured, commonly used and machine-readable format and to transmit that Personal Data to another entity.
- **Right to make a complaint:** without prejudice to any other administrative or judicial dispute, if Data Subjects believe the Processing of Personal Data has been carried out illicitly or not in compliance with Applicable Data Protection Laws. Data subjects have the right to raise a complaint with the Supervisory Authority of the Member State or country in which they reside or work habitually, or of the State or country where any breach has allegedly occurred.
- **Right to Opt-Out of Sale:** right to opt-out of the sale of Personal Data. Sales encompasses any sharing of data for value (monetary or otherwise). Westinghouse does not sell Personal Data.
- **Right to Restrict Use of Personal Data:** right to opt-out only applies to Sensitive Personal Data that is used for the purpose of inferring characteristics about the employee.
- **Right Against Retaliation:** employers cannot retaliate against employees, job applicants, contractors, if any employee chooses to opt-out or exercise of their other rights.





## 11.0 Guidelines to Westinghouse Representatives

Employees, agents, representatives and contractors (collectively "**Westinghouse Representatives**") must comply with this Policy when Processing Personal Data on Westinghouse's behalf.

We recognize that Personal Data loss or misuse may sometimes result in harm to individuals, including embarrassment, inconvenience, and fraudulent data use. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that Westinghouse always takes seriously.

Based on the definitions and principles provided herein, Personal Data shall be processed in accordance with the following guidelines:

- Westinghouse Representatives may only access Personal Data when performing their job duties requires such access. To safeguard the integrity of Personal Data, access to Personal Data is granted on a need-to-know basis, limited only to Westinghouse Representatives who need access to such data in order to do their job. Westinghouse does not permit access to Personal Data for any other reason.
- Personal Data must be processed legally, fairly, and confidentially.
- Westinghouse Representatives must exercise particular care when processing Sensitive Personal Data, since they relate to fundamental rights and freedom of the Data Subjects and the relevant loss and misuse may cause significant damage to the Data Subjects.
- Please contact the Global Compliance Organisation if you: (1) are unsure whether a specific use is appropriate, (2) have any questions regarding the privacy notices that apply to collected Personal Data, or (3) need to obtain an approved privacy notice before Processing Personal Data.
- Personal Data collected shall be accurate and kept up to date and relevant to the purpose for which it was collected. To the extent practicable, the Westinghouse Representative shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Westinghouse Representatives will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.
- Personal Data shall be stored as long as it is necessary to pursue the purposes for which it was collected. Westinghouse Representatives shall immediately inform the Global Compliance Organisation if they come across Personal Data that may not, or no longer, be necessary (e.g., Personal Data of former employees who have left the Company more than 10 years ago), or if they suspect that Personal Data may be retained in breach of the any applicable retention policies.
- Westinghouse Representatives may only share Personal Data with another Westinghouse Representative if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions. If you are unsure about whether a specific disclosure is appropriate or allowed, you must consult with the Global Compliance Organisation.

## LEGAL

**Personal Data Protection and Privacy Policy**


---

- Cross-border transfers of Personal Data (including transfers among Westinghouse entities) are subject to restrictions and specific rules aimed at ensuring that Personal Data are always adequately protected. Westinghouse has put into place the necessary transfer mechanisms to enable the lawful use of Personal Data among Westinghouse entities, while Westinghouse Representatives must consult with the Global Compliance organisation to ensure that any cross-border transfer is approved.
- Westinghouse Representatives are responsible for protecting the Personal Data the Company holds. Representatives must comply with all applicable aspects of Westinghouse Information Security Policies and must comply with and not attempt to circumvent the administrative, physical, and technical safeguards the Company implements and maintains in accordance with Applicable Data Protection Laws. Westinghouse will develop, implement, and maintain safeguards appropriate to its' size, scope and business, its' available resources, and the amount of personal data that the Company owns or maintains on behalf of others, as well as attempt to safeguard against identified risks.
- If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact the Global Compliance Organisation and the Information Security organisation. You should preserve all evidence relating to the potential security incident.
- Data Subjects may have rights when it comes to how we handle their Personal Data. These rights vary depending on the where the Data Subject resides but may include the right to obtain access to or copies of Personal Data; to have inaccurate or incomplete information corrected; and in some cases, have the right to request that the Company erases or stops using certain data; as well as the right to object to the processing of Personal Data. You must immediately forward any Data Subject request you receive (either in writing or verbally) to the Global Compliance Organisation.
- Any new Westinghouse initiative/activity/process/tool/application entailing any Processing of Personal Data and any initiative/activity/process/tool/application entailing the use of Personal Data for new or different purposes, shall be submitted to the verification and validation of Global Compliance Organisation, to ensure that grounds for lawful processing exist.
- To exercise any of the rights granted to Data Subject, to report Security Incidents, to ask questions about this Policy or any privacy notice, or for any query or further clarification or instructions on the processing of Personal Data, please contact the Global Compliance Organisation at:
  - Email address: [dataprivacy@westinghouse.com](mailto:dataprivacy@westinghouse.com)
  - Mailing address: Ethics and Compliance, Westinghouse, 1000 Westinghouse Drive, Cranberry Township, PA 16066, USA

## 12.0 Revision Summary

Revision	Section	Revision Description
0	All	Initial Issue



LEGAL

## Personal Data Protection and Privacy Policy

---

1.0	All	Overall review and updates
2.0	All	Annual review and updates
2.1	All	Minor format edits and annual refresh

\*\*This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.\*\*

## Approval Information

Author Approval Brown Gary Jul-01-2024 04:23:12

Approver Approval Harsch Nathan Jul-01-2024 07:54:07

Files approved on Jul-01-2024

\*\*\* This record was final approved on 07/01/2024 07:54:07. (This statement was added by the PRIME system upon its validation)