Vistra data protection framework

Vistra believes that a strong business reputation depends on a robust data protection and information security framework. We view data protection and information security as fundamental components of doing business. We are committed to protecting information assets, personal data, and client information.

Our data protection framework

We have developed a comprehensive data protection program using global privacy standards to ensure we meet our obligations across the countries and regions where we operate. Our policies and procedures are built on a strong foundation of internationally accepted privacy principles of transparency, accountability, and individual rights, including the General Data Protection Regulation (GDPR) and other regional privacy laws and regulations. We seek to continuously improve and enhance our framework, upholding high standards in collecting and processing personal data across our business practices and services.

Key aspects of our data protection framework

We have a suite of data protection and information security policies and procedures to meet the requirements and standards of applicable data protection laws, including:

Data protection

Our data protection policies apply to all Vistra office locations and all our employees, contractors, vendors and third parties. Our accountability and governance measures ensure that we understand and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.

Data incident management

Our data security procedures ensure that we have safeguards and measures in place to identify, assess, investigate, and report any personal data breach in line with regulatory expectations.

Data retention

Our retention policies and practices are designed to ensure that we meet the ‘data minimization’ and ‘storage limitation’ principles and that personal data is stored, archived, and destroyed compliantly and ethically. We have dedicated procedures in place to meet the data subject’s rights and are aware of when data subject’s rights apply, along with any exemptions, response timeframes, and notification responsibilities.

International data transfers

We leverage a global infrastructure and enjoy the provision of 24/7 support that may require data to be stored in centralized locations across borders. Where this is the case, we have taken steps to guarantee the correct safeguards are in place to allow for data transfers and ensure we meet the compliance obligations set out in applicable data protection laws. For example, where appropriate, EU approved Standard Contractual Clauses are incorporated within our client and supplier contracts to extend GDPR rights and safeguards accordingly. Where Vistra stores or transfers personal data outside the EU, we have appropriate procedures and additional safeguarding measures in place to also secure, encrypt and maintain the integrity of the data.

v.2024.1 (Owned by the Group Data Privacy Officer)

Training and awareness

We have a mandated employee training program that is provided to all employees upon hire and annually thereafter. Ongoing privacy awareness communications and activities are conducted often, and specialized training sessions are provided for specific roles or departments as appropriate.

Privacy notices

We provide privacy notices to individuals to inform them why we need their personal data, how it is used, what their rights are, to whom the information is disclosed, and what safeguarding measures are in place to protect their information.

Privacy impact assessments (PIA)

We have developed procedures and templates for carrying out privacy impact assessments that comply with the applicable data protection laws. We have processes in place to assess risk when we process personal data that is considered high risk, involves large-scale processing, and/or includes special category data.

Processor agreements

Where we use any third party to process personal data on our behalf, we have drafted compliant processor agreements and due diligence procedures for ensuring that they (as well as we) meet and understand their/our data protection obligations.

Information security, technical and organisational measures

Vistra takes the privacy and security of personal data very seriously and has implemented administrative, physical, and technical safeguards to protect and secure the personal data that we process. We have established policies, procedures, governance processes, and technical requirements where applicable to manage IT security risk across the business with key security and data protection regulations, standards, and frameworks.

Vistra prioritizes the privacy and security of personal data through a robust framework that include a blend of administrative, physical and technical safeguards. Our comprehensive security strategy is aligned with international standards such as National Institute of Standards and Technology (NIST) and International Organization of Standards (ISO) 27001:2013, ensuring we adhere to the highest level of data protection. Key measures encryption, strict access control, secure coding practices and ongoing employee training. These efforts are underpinned by regular policy review and governance processes to manage IT security risks effectively.

You may find further details in the webpage below on the security measures we have in place to safeguard your personal data: https://www.vistra.com/security.

Information security audits

To provide us with a more complete view of our information security compliance, our services and infrastructure are subject to regular audits. We conduct several forms of audit:

- annual independent third-party compliance audits against ISO 27001:2013 to certify that the Information Security Management System (ISMS) employed within our global data centers and core corporate systems meets global standards
- monthly IT Environment vulnerability scans, which focus on the technical aspects of our Global Information Security Policy, such as patch management, application security, and infrastructure security.

Data privacy team

Vistra has a dedicated data privacy team to oversee our privacy program and ensure its continued success. The data protection regulatory environment remains dynamic and subject to new regulatory action. Vistra stays in touch with these changes through conferences, industry associations, and our contacts within key government agencies, so that we remain in compliance and continue to be a constructive partner.

If you require further information regarding our data protection framework, you can contact the Data Privacy team by emailing: privacy@vistra.com.

In summary

Vistra secures the information assets of our clients by adhering to a global data protection and information security framework. Our global applications and systems are subject to both privacy impact assessments and security certification reviews, which support a robust, consistent approach in deployment and operation. We protect personal data within our network using appropriate physical, technical, and organizational security measures. We confirm that our contracts with third-party processors contain provisions that are commensurate with our own policies, practices, and controls to confirm that your data is managed properly and securely in accordance with legal and regulatory requirements. Clients and individuals rightfully demand accountability from any organization handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information assets and are committed to protecting your data. If you have any questions or require further information on how we protect you and your business, please contact your Vistra representative.

v.2024.1 (Owned by the Group Data Privacy Officer)