West Privacy Program

Privacy and Data Protection Mission Statement

West Corporation and its affiliates ("West") take seriously the obligations to protect personal information provided by its customers. West will use such information only for the purposes for which it is provided. As a leading global services provider, West ascribes to principles of privacy in the protection of customer personal information that transcends legislative requirements and meets and exceeds the legal obligations defined in each of its global locations in every region of the world. West routinely reviews, updates and expands its privacy policies to ensure adequate protection for its broad support of customer personal information around the world.

LEGAL AND REGULATORY COMPLIANCE

At all times, West ensures compliance with privacy and data protection laws in the United States and Canada (including but not limited to the Gramm-Leach-Bliley Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and Canada's Privacy Act), the United Kingdom (including the Data Protection Act), the Asia-Pacific region (including but not limited to Japan's Act on the Protection of Personal Information, Australia's Privacy Act along with the Australian Privacy Principles, Singapore's Personal Data Protection Act and Hong Kong's Personal Data (Privacy) Ordinance), the European Union (including GDPR and EU member state legislation) and anywhere applicable around the world.

West Privacy Program

- Mission Statement
- Legal and Regulatory Compliance
- Privacy Team
- Training and Audits
- Third Party Management
- Data Integrity
- Customer Privacy Policy
- Security
- Privacy and Security Risk Management
- Data Inventory
- Data Retention
- Categories of Personal Information Processing
- Purpose of Processing
- GDPR Compliance

PRIVACY TEAM

West has a dedicated privacy and data protection team. The team is comprised of lawyers and privacy practitioners, many of whom are certified privacy professionals. The team is spread across the world and assists on privacy and data protection matters with global customers. The team fosters a data protection culture among employees and communicates personal data protection policies to stakeholders. Additionally, the team helps to ensure West is compliant with data protection legislation and manages data protection related complaints and queries.

TRAINING AND AUDITS

West provides its employees with regular mandatory privacy and security training and awareness. Such training and awareness outlines the processes and procedures for protecting data, information, and information systems. Attendance and comprehension are tracked.

West conducts regular risk assessments and privacy impact assessments. The objective of a privacy impact assessment is to assess West's privacy protection position against any legislative/contractual requirements or international best practices and to review compliance with West's own privacy-related policies. The scope involves evaluating procedures undertaken by West throughout the typical information life-cycle phases: how information is created or received, distributed, used, maintained and disposed of or deleted.

THIRD PARTY MANAGEMENT

West does not share information with third parties unless that transfer of information is necessary for completion of required business operations and, at all times, complies with relevant law and privacy regulations.

Third parties acting on behalf of West are subject to written nondisclosure agreements with West and are required to comply with West's privacy policies and processes. Such contractors of West are responsible for adhering to the approved information security policies and procedures. Violations of the information security policy are subject to penalizing action up to and including termination of the relationship between West and the contractor. Third parties will be asked to commit to these obligations via contract.

DATA INTEGRITY

West only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized by a customer. To the extent necessary for those purposes, West takes reasonable steps to ensure personal information is accurate, complete, current and reliable for its intended use. West provides customers the opportunity to correct inaccuracies in the personal information it retains and delete personal information upon a customer's request, unless the burden or expense of providing access would be disproportionate to the risks to a customer's privacy or where the rights of a customer would be violated.

CUSTOMER PRIVACY POLICY

West has extensive customer privacy statements, which are found at www.west.com/legal-privacy/

SECURITY

West is committed to protecting its customers' personal information. West implements physical, administrative and technical security measures. Despite such efforts, if West learns of a security breach involving a customer's personal information, when required by law or contract, West will notify the affected customer so appropriate protective steps can be taken. West is not responsible for unauthorized access to such personal information by hackers or others that obtain access through illegal measures, in the absence of negligence on the part of West. West's information security policy incorporates the ISO 27002 information security standards. Many of West's data centers are ISO27001 certified.

Some of West's business units comply with other information security and privacy standards that include but are not limited to:

- Payment Card Industry Data Security Standard
- Gramm-Leach Bliley Act
- Health Insurance Portability and Accountability Act
- Federal Information Security Management Act
- EU Standard Contractual Clauses
- Privacy Shield

PRIVACY AND SECURITY RISK MANAGEMENT

West conducts privacy and security risk management at various levels to address the needs of evaluating the systems and functions of its various business units. At the highest level, West's Enterprise Privacy and Security Board meets to set policy and address corporate-level privacy and security issues. Advising this board are the Enterprise Information Security and Privacy groups.

DATA INVENTORY

Customer personal information may be processed by West, its affiliates and contractors in the United States, the United Kingdom, the European Union and the rest of the world and may be transferred outside the country in which a customer provided such personal information. West acts as a "Data Processor" in relation to the personal information from customers or on behalf of customers, and each customer remains the "Data Controller" with respect to such personal information.

West has operations, facilities, call centers and sales offices in over 20 countries across the Americas, Europe and Asia-Pacific. Depending on the services used, the services set up, services mix and the geographical location of the users, West's affiliates may be used to provide services to customers.

Global Infrastructure and Operations Centers:

• Americas: USA, Canada

• EMEA: United Kingdom, France, Germany, Sweden

• APAC: Australia, China, Hong Kong, India, Japan, Malaysia, Philippines, Singapore

Sales and Administrative Offices:

• Americas: USA, Canada, Mexico, Brazil

• EMEA: United Kingdom, Belgium, Denmark, Finland, France, Germany, Israel, Italy, the Netherlands, Spain, Sweden

• APAC: Australia, China, Hong Kong, India, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea

DATA RETENTION

Customers' personal information is not kept for longer than is necessary to accomplish the purpose for which it was collected. West undertakes to do the following:

• Review the length of time it retains personal information;

• Securely delete personal information no longer needed for a specific purpose; and

• Update, archive or securely delete personal information if it becomes out of date.

CATEGORIES OF PERSONAL INFORMATION PROCESSED BY WEST

Personal information related to users, as necessary for the delivery and invoicing of West's services, may include:

• First name and last name;

• Telephone and fax numbers, job title, e-mail address and similar communication data;

• Access and connection data in relation to the use of the services;

• Codes, account numbers, pass codes in relation to the delivery of the services;

• Recordings and transcriptions, as requested by a customer;

• Financial and creditworthiness information, bank account details, credit card information;

• Cost codes, files references and other references requested for invoicing and internal administration purposes;

• Information provided for monitoring, training, coaching and quality purposes; and

• Other data required pursuant to statutory provisions and other information voluntarily disclosed by the users through the use of the services.

PURPOSE OF PROCESSING

The processing of personal information is made for some of the following purposes to the extent it is required for the delivery of West's services:

• Services set up and delivery:

• Support, maintenance and resolution of users' queries;

• Account set-up and account management;

• Invoicing and collections purposes;

• Records and internal administration;

• Business reporting and statistical analysis;

• Complying with legal obligations; and

• Cooperating with respect to actual or prospective legal proceedings, inquiries and investigations of governmental, judicial or regulatory authorities.

GDPR Compliance

West is a data processor in relation to its handling of European Union customer personal data. There are a number of obligations on West under GDPR. West put in place a comprehensive GDPR compliance program that, among other things, specifically includes privacy by design, privacy impact assessments on our services, data mapping, privacy audits, updating our customer contracts and training videos, retention policies, data minimization, data accuracy, record keeping, access rights, security, meeting ISO27002 standards, notification policies and ensuring our sub-processors meet our privacy and security minimum standards.

Last revised in January 2019