WEST GDPR COMPLIANCE GUIDE

This document outlines some of West's core compliance processes with the General Data Protection Regulation ("GDPR").

INTRODUCTION

The GDPR applies to any business that acts as data controller or data processor and that offers goods or services to individuals in the European Union ("EU"), regardless of whether it is physically located in the EU. West and its affiliate companies that process personal data of individuals in the EU ("West" or "we") has implemented the measures outlined in this document.

Under GDPR, West acts as a "data processor" in relation to the personal data from customers or on behalf of customers, and each customer remains the "data controller" with respect to such personal data. There are a number of obligations on data processors under GDPR. Accordingly, West has a comprehensive GDPR compliance program that will, among other things, outline West's processes in relation to demonstrating compliance (privacy by design, privacy impact assessments on our services, data mapping, privacy audits, updating our customer contracts and training videos), retention policies (data minimisation, data accuracy and record keeping and access rights), security (ensuring accuracy and meeting ISO27002 standards), notification policies (breach notification procedures) and subcontracting (ensuring our subcontractors meet our privacy and security minimum standards).

PROCESSING PERSONAL DATA

West conducts privacy impact assessments on its services, systems, platforms, databases, processes and vendors. We keep records of data processing activities, a personal data inventory and we incorporate policies such as data minimisation, privacy by design and pseudonymisation into our privacy processes.

West integrates data privacy into its information security policy by including storage and limitation, encryption, integrity and confidentiality, breach notifications and transparency. West implements regular security risk assessments, data quality procedures, tools for data de-identification and an encryption policy. We have policies and procedures to ensure personal data is accurate and kept up to date. For data that is inaccurate, the data is erased, updated or otherwise rectified.

West obtains valid grounds for processing personal data from customers via customer contracts, order forms and/or website terms and conditions. We keep an internal database of executed contracts and order forms and maintain a data inventory that sets out what ground is relied on when processing personal data.

DATA BREACH NOTIFICATION PROCEDURES

West has data breach notification procedures to ensure it notifies customers where required and in accordance with GDPR and customer contract obligations. Documentation that outlines West's data breach notification procedures and incident response plan is available upon request.

West has a breach response plan that ensures compliance with Article 33 of GDPR in respect of timing requirements for notification and the content of a notification letter. The breach response plan maintains a log to track data breaches. West conducts data breach response testing and we maintain data breach metrics.

PRIVACY STATEMENT

West has a privacy statement that details our personal data handling processes. The privacy statement is an external-facing notice of West's processing activities. It further ensures that the required information is provided to data subjects when their information is collected such as secondary uses of personal data.

The privacy statement addresses the following:

- How West can respond to access requests in a timely and appropriate manner;
- Purpose of processing personal data;
- Categories of personal data;
- Recipients of personal data;
- Data storage periods;
- Rights to rectification and complaint;
- Sources of data; and
- Safeguards for transfer to third countries.

RIGHT TO BE FORGOTTEN, CORRECTIONS AND PORTABILITY

West has procedures to respond to requests to be forgotten or for erasure of data. West ensures to delete personal data on the grounds of data is no longer necessary for processing unless we are required to retain the data for a longer period of time as required by applicable law. We have processes in place to ensure that records of personal data are used in line with any restrictions, and respond to requests to opt-out, restrict or object to processing. West has a data retention policy that is available upon request. It outlines times on the erasure or pseudonymisation of customer personal data.

Customers' personal data 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 data;
- Securely delete personal data no longer needed for a specific purpose; and
- Update, archive or securely delete personal data if it becomes out of date.

West maintains procedures to respond to requests to update or correct customer personal data, as well as having technical solutions in place for processing data portability requests.

AUDITS AND PRIVACY IMPACT ASSESSMENTS

West has implemented appropriate technical and organisational measures to ensure and be able to demonstrate compliance with GDPR. These measures include but are not limited to privacy impact assessments and data mapping of products, solutions, databases and projects ("PIAs"), annual internal privacy audits, data inventory lists, data breach assessments and information security testing (together, "Audit Measures").

Audit Measures are taken on certain new programs, products, systems, databases and processes. West engages internal stakeholders from relevant departments when conducting Audit Measures, which take into account the following:

- A description of the processing activities being assessed;
- An assessment of the risks to data subjects; and
- A description of the measures West takes to address risks, including safeguards, security measures and mechanisms that West will implement to ensure GDPR compliance. Data protection issues or risks are then tracked and addressed.

The objective of a PIA is to assess West's privacy protection position against any legislative, contractual requirements and international best practices and to review compliance with West's own privacy policies. The scope of a PIA involves evaluating procedures undertaken by West throughout

the typical information life-cycle phases: how data is created or received, distributed, used, maintained and disposed of or deleted.

Audit Measures guarantee that data protection risks are measured, analysed and mitigated and they enable West to identify issues and risks and determine, based on the likelihood and impact, where to prioritise resources to mitigate risk. Audit Measures also ensure the ability for West to demonstrate that appropriate technical and organisational measures have been put in place for compliance with GDPR.

PRIVACY BY DESIGN

West integrates privacy by design into our systems and product development. Examples of privacy by design include application development protocols, security risk assessments, software for aggregation, data masking and pseudonymisation, encryption and anonymisation. West implements data protection by default into our security, product and operational processes.

West anonymizes personal data in which direct and indirect personal identifiers are removed and technical safeguards are implemented such that the personal data can never be re-identified so there is zero re-identification risk.

In some cases, West pseudonymzes or encrypts processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

SUB-CONTRACTING AND THIRD PARTY VENDORS

West only appoints sub-contractors that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and with a contract that governs the relationship. We provide information security and privacy screening questions for potential sub-contractors and other processors, as well as maintaining lists of sub-contractors that process our personal data, which are available to customers, employees and supervisory authorities upon request.

West appoints sub-contractors under a binding written agreement, which requires that sub-contractors only act on West's instructions and ensure the security of West's personal data that it processes. At a minimum, West's binding written agreement stipulates that sub-contractors must:

- Only act on West's documented instructions;
- Impose confidentiality obligations on all personnel who process the relevant data;
- Ensure the security of the personal data that it processes;
- Not send personal data to third party suppliers or impose the same data protection obligations on its third party suppliers without our approval; and
- Implement measures to assist West in complying with the rights of data subjects.

West conducts regular due diligence, audits and assessments on its sub-contractors to ensure compliance with GDPR and general data protection and security obligations. West's sub-contractors are required to keep personal data that they process confidential.

SECURITY

West implements physical, administrative and technical security measures. If West learns of a security breach involving personal data, when required by law or contract, we notify the affected customer so appropriate protective steps can be taken. West is not responsible for unauthorized access to such personal data 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 framework.

The following security measures are implemented by West:

- encryption of personal data at rest and in transit;

- technical security measures such as intrusion detection, firewalls and monitoring;
- on-going tests and reviews of security measures;
- redundancy and back-up facilities;
- processes to restore availability of and access to personal data in the event of an incident;
- password parameters, data centre security measures, identity access management and restrictions on accessing personal data;
- audits and tests on information on West's internal security processes and West's sub-contractors information security processes;
- information security incident/breach response plan; and
- data logging to track all data privacy incidents and breaches.

West has a dedicated information security team that assists the business globally.

DATA PROTECTION OFFICERS AND REGISTRATION WITH A SUPERVISORY AUTHORITY

West has a designated data protection officer ("DPO") in order to comply with Article 37 of GDPR. Steven Taylor is West's DPO and his contact details are noted below. Additionally, West has a dedicated privacy and data protection team of legal professionals ("Privacy Office") that are responsible for West's compliance with applicable data privacy legislation and contractual obligations. The Privacy Office may be contacted via email at privacy@west.com.

For the purposes of GDPR compliance, West's lead supervisory authority in the EU is the Information Commissioner's Office in the United Kingdom.

CROSS BORDER DATA TRANSFERS

Customer personal data may be processed by West, its affiliates and sub-contractors in the United States, the United Kingdom, the European Union, Canada, Mexico, India, Philippines and the rest of the world and may be transferred outside the country in which a customer provided such personal information.

West's PIAs and data mapping maintain logs and records of the personal data transfers. The basis for such transfers include but are not limited to:

- services reservation, set up and delivery, pre and post-call services;
- support, maintenance and resolution of customer queries;
- account set-up and account management;
- invoicing and collections purposes;
- records and internal administration;
- business reporting and statistical analysis;
- complying with legal obligations of the data exporter and/or the data importer; and
- cooperating with respect to actual or prospective legal proceedings, inquiries and investigations of governmental, judicial or regulatory authorities.

West complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and Switzerland to the United States, respectively. West and its affiliates also use standard contractual clauses as a data transfer mechanism.

GDPR TRAINING

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

CONCLUSION

West proactively monitors future developments in EU and global privacy laws, including best practices. West may at any time update or modify its privacy and data security processes. The information contained herein has been prepared for general information purposes only to permit you to learn more about West's privacy and data protection processes. The information presented is not legal advice, is not to be acted on as such, may not be current and is subject to change without notice.

NEED MORE INFORMATION?

Contact your dedicated Account Manager, or regional retail team:

NORTH AMERICA
westuc.com | +1-800-232-0900

EUROPE, MIDDLE EAST & AFRICA
westuc.com |
conferencingEMEA@west.com

ASIA PACIFIC
westuc.com |
cserviceAPAC@west.com

You may also contact privacy team members from West's legal department:

NORTH AMERICA

Janette K. Nelson
jknelson@west.com

EUROPE, MIDDLE EAST & AFRICA
AND ASIA PACIFIC

Steven T. Taylor
steven.taylor@west.com