Privacy and Data Protection Policy

AMARILLO BROKERAGE COMPANY

Amarillo Brokerage Company, LLC

Amarillo Brokerage Company's Privacy and Data Protection Policy

Introduction

In the course of our business, we process data, including personal, for a wide range of purposes such as employment, marketing, management, the performance of services to our clients. To protect personal data, we are required to comply with various data protection principles. This Privacy and Data Protection Policy ("**Policy**") sets out groupwide data protection principles and commitments that Amarillo Brokerage Company adheres to. It also sets out roles and responsibilities and provides procedural guidance for when Amarillo Brokerage Company locations need to deviate from the global principles and commitments in order to meet the local legal requirements.

Contents

1. Definitions

"**Applicable Law**" means any applicable data protection related laws and regulations within the UK/EEA, as amended, extended or re-enacted from time to time, including but not limited to the following: (i) EC Regulation 2016/679 (the "**GDPR**") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; (ii) the GDPR as incorporated into UK law (the "**UK GDPR**") pursuant to Section 3 of the European Union (Withdrawal) Act 2018; (iii) the UK Data Protection Act 2018; (iv) EC Directive 2002/58/EC on Privacy and Electronic Communications; (v) all local laws or regulations implementing or supplementing the legislation mentioned above; and (vi) all codes of practice and guidance issued by national regulators relating to the laws, regulations mentioned above. In the scope of the "Applicable Law" are also the other privacy laws, which apply to Amarillo Brokerage Company, such as the Singaporean Personal Data Act of 2012 (PDPA); The Brazilian General Data Protection Law (LGPD); and the Hong Kong's The Personal Data (Privacy) Ordinance and any other applicable national law implementing data protection in a jurisdiction Amarillo Brokerage Company is operating in. Further details are in the Annexure of this Policy.

"**Personal Data**" is all information which, either alone or in combination with other information we hold, can identify an individual. It includes not only facts, but also intentions and opinions about the person.

"Processing" means any operation which is performed on personal data. It includes the whole lifecycle of using the data from collecting it, holding it, disclosing it to deleting it, whether this is done manually or by automated means.

"Data Subject" is any natural personal who can be identified by reference to his/her personal data.

"Third Party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"Unstructured Data" is any data which is not stored in an organised structure and not processed through predefined datasets.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Where this Policy refers to **"Amarillo Brokerage Company", "company", "we", "us" or "our",** this means one or more of the Companies.

2. GDPR as the Gold Standard

Amarillo Brokerage Company sets out the General Data Protection Regulation as the Gold Standard for the processing of personal data. Consequently, the basic rules and the principles of the GDPR are used as a norm with the expectation of the local entities to adhere to the same standard of data protection. Deviations from the Gold Standard, which may arise from non-EEA privacy legislations, regulations or business requirements are considered and appropriately documented and approved by the Privacy Team for any operations of the company involving personal data in these jurisdictions.

3. Amarillo Brokerage Company's global privacy commitments according to the data protection principles

Every member of the staff is required to familiarise themselves with and accordingly follow the data protection policies, procedures. For more information see the Data Protection Framework and the Data Protection – Staff Responsibilities Policy.

As an organization that processes personal data, we must globally comply with certain data protection principles and therefore Amarillo Brokerage Company is committed to:

- **Use personal data lawfully, fairly, transparently and only for a valid purpose:** Amarillo Brokerage Company ensures that every collection and further processing of personal data is based on **appropriate legal grounds** and also that the data is processed **transparently** and in a way that individuals would reasonably expect. By **appropriate legal grounds**, we mean that we have a clear and identifiable lawful basis and **purpose** for the collection and that we only process the personal data according to the same. Complying with the **fairness** principle means we ensure to process data in a manner, which is fair and reasonable and can be expected by the data subject. By **transparent**, we mean that we provide clear and accessible information about the personal data we collect, why we collect it, what we use it for, who we disclose it to, and how long we keep it for.

For more information see Amarillo Brokerage Company's Employee Privacy Notice, Client and Website Privacy Notice and the Recruitment Privacy Notice

- **Use accurate, minimal and up-to-date personal data:** By maintaining robust and regularly reviewed record keeping processes and systems, Amarillo Brokerage Company keeps personal data precise and complies with the legal obligations on accuracy. We also use the minimal amount of data needed to achieve the legitimate purpose. The data is kept in adequately approved applications in order to mitigate the amount of unstructured data and unnecessary duplicates within the company.

- **Keep the data only as long as necessary for the legitimate purposes:** Amarillo Brokerage Company keeps personal data for no longer than is necessary and only for reasons that were disclosed to the individual prior to the processing of personal data. To comply with the principles, all locations must follow the Erasure controls as defined in the erasure processes. These clarify the steps for defining the retention triggers and times which must be implemented into the business processes to comply with the requirements on storage and the deletion of personal data throughout its lifecycle.
  For more information, see Amarillo Brokerage Company's Retention Criteria Capture Process and Retention Erasure Planning Process.

- **Implement appropriate technical and organizational measures with privacy as the default:** Amarillo Brokerage Company has implemented a relevant policy, contractual and technological measures to minimize the risk of breaches and other privacy incidents leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. We only disclose data to other parties where we have a justifiable reason to do so and where we are satisfied that the other parties can sufficiently guarantee the security of the data. Amarillo Brokerage Company will integrate the necessary safeguards by design and by default into any uses or other processing of personal data in accordance with the applicable law.
  For more information, see Amarillo Brokerage Company's Information Classification and Handling Policy and Acceptable Use Policy. You are also required to familiarize yourself with all the relevant information security policies and follow these in practice.

- Implement **third party engagement processes**, which ensure the data transfers from Amarillo Brokerage Company to a Third Party are secure, and compliant with the applicable privacy laws. We must not disclose personal to persons outside of Amarillo Brokerage Company unless it is known that they are authorized to receive it and have a proper purpose of processing. Before any personal data is sent out from the Amarillo Brokerage Company's infrastructure, the Third Party receiving the data must go through a vetting process internally. The person seeking to engage a vendor or send personal data to another entity, must raise a request in PeopleSoft for the relevant sign-offs. Where staff are unsure how best to Process data, receive an unusual request from an unusual source or have any other queries about the Processing of data, they must contact our DPO or the Privacy Team. For more information see the Contract Request – Supplier DB Quick User Guide and Privacy Vendor Onboarding Policy.

- Manage **data breach and incidents with appropriate** responses, including making necessary notifications to regulators and data subjects. All the staff are required to follow the Data Breach Policy and personal data breaches and incident must be reported to the Group's Privacy Team and the DPO at mike@amarillobrokerage.com without delay. Any personal data breach reporting, investigation and mitigating actions is a priority.
  For more information see Amarillo Brokerage Company's Data Breach Policy and Data Breach Reporting Form.

- **Conduct a Data Protection Impact Assessment (DPIA) to assess the risks in the applicable processes:** Where a type of use or collection is likely to harm the data subjects, the BPO and/or AO is required to complete a DPIA according to the internal process to assess the impact of the intended use or collection

on the individuals and to mitigate the associated risks in accordance with the applicable laws and the internal controls.

For more information, see Amarillo Brokerage Company Privacy Risk Assessment Policy.

- **Facilitate the exercise of the Data Subject Rights:** Amarillo Brokerage Company ensures to share with the data subjects all the necessary information about their rights and to provide simple, clear and straightforward instructions for their exercise as the applicable legislations require.
  For more information see Amarillo Brokerage Company's Data Subject Right Request Manual.

- There are exceptional situations where the business requirements make it necessary to depart from an approved policy, procedure or process which heightens the operational risk. In these circumstances, the firm can choose to accept this risk and formally request an acceptance by following a **Risk Acceptance Procedure**. To initiate a risk acceptance request, you must do so in the Self Service Portal. Alternatively, you can contact the Change Risk & Assurance team at mike@amarillobrokerage.com.

- Amarillo Brokerage Company recognizes that the protection of Personal Data can only be achieved when our entire global staff is aware of and take steps to comply with our global data protection commitments. As such, Amarillo Brokerage Company provides **data protection training and support** to all our staff, who are required to complete the relevant training within the deadlines, and implement the lessons learned into the daily work.

4. Responsibilities

Everyone at Amarillo Brokerage Company is required to comply with our data protection responsibilities and must act in accordance with the data protection principles. When processing personal data, Amarillo Brokerage Company is generally the **Controller** of the personal data and hence responsible for determining the purposes and the means of the processing. However, there are cases in which Amarillo Brokerage Company cooperates with other Controllers and inevitably share with them specific types of personal data according to the relevant privacy legislations. When Amarillo Brokerage Company transfers personal data to a service provider in order to process it on its behalf, the service provider will be considered to be a **Processor.**

Our **Board**, the **Executive Management team** and **Regional Heads** have the overall responsibility to ensure we have the necessary governance, management applications and tools in place to meet our data protection responsibilities. They are also responsible for promoting a privacy inclusive culture within the business by supporting the business to choose processes which are compliant with the legal privacy frameworks.

Business Process and Application Owners are responsible for implementing the Privacy Principles and controls into their processes and applications, undertaking data protection impact assessments, assisting in data subject rights responses and playing an active role in breach investigations and Data Subject Right responses. Business Process and Application Owners are also responsible for setting and maintaining data access controls within the processes and applications they manage.

The **DPO** with the help of the **Privacy Team** is responsible for creating, revising and maintaining the privacy compliance framework and keeping records of its activities. They are also responsible for supporting the business by advising and educating our teams, staying up to date with legal and regulatory developments and providing alerts to affected departments. The DPO must interact with the data protection regulators where applicable.

5. Local requirements and seeking support

This Policy sets out Amarillo Brokerage Company's global approach to privacy and data protection compliance. It sets a baseline standard that Amarillo Brokerage Company adheres to in all its global locations and is designed to ensure compliance with the privacy and data protection laws and regulations.

In recognition of the global deviations in the privacy laws, Amarillo Brokerage Company had developed a non-UK/EEA Privacy Programme and Rollout Plan. Please see the Annexure for more detailed information.

6. Ongoing Review

The DPO and Privacy Team, working in conjunction with the Business Process and Application Owners and the Senior Management, will perform a periodic evaluation of specific data privacy controls against the major legal, regulatory and policy requirements. Results of the periodic evaluation will used to improve data protection systems and controls across the business.

7 Changes to This Policy

This Policy will be reviewed annually an as per needed, in particular in the context of each non-EEA jurisdictional privacy roll-out. The Policy is approved by the Regional Heads and the Head of Risk and presented to the Audit and Compliance every 3 years or after a material update. This Policy was last reviewed in November 2023.

8. Contact

Please contact our Group Data Protection Officer (GDPO) or our Privacy Team at mike@amarillobrokerage.com with any questions on this Policy our data protection obligations generally.

Annexure – Information specific to Amarillo Brokerage Company jurisdictions

In recognition of the global deviations in the privacy laws, Amarillo Brokerage Company had developed the following non-UK/EEA Privacy Programme and Rollout Plan:

1. The Privacy Team in cooperation with other relevant stakeholders prioritise non-UK/EEA jurisdictions based on the scope of the local operations, the high-level privacy framework of each jurisdiction and the level of risk where compliance is not achieved.
2. The Privacy Team will document a "gap analysis" to assess the differences between data protection laws in the UK/EEA and the local data protection laws.
3. The gap analysis will be sent for an external validation to (a) local counsel(s).
4. The Privacy Team will work with other relevant stakeholders to document data maps in OneTrust (privacy software). This is achieved as far as possible by automation and training the business in the use of OneTrust.
5. A local contact point will take the lead in driving the actions further within the local Amarillo Brokerage Company business. This may be (for example) a local privacy external business or a nominated Amarillo Brokerage Company privacy manager. The specific model is dependent on the budget, risk-appetite of Amarillo Brokerage Company and available resources.
6. The Privacy Team conducts a gap analysis evaluating the data maps against the externally validated legal framework.
7. The Privacy Team estimates whether the existing EEA/UK data protection law controls are suitable to close the local privacy "gaps". This estimation considers:
    1. compliance with the legal requirements;
    2. the practicability for the business processes and applications.
8. Any deviation from the existing EEA/UK data protection law controls must be justified and documented by the local entity and approved by the Group's relevant stakeholders, including the DPO. The documented justification and the deviating controls are stored with the Privacy Team.
9. Local contact points are responsible for the ongoing implementation and the maintenance of the necessary controls. The Privacy Team will assist in directing the operations.
10. Compliance and local law firms will assist in identifying major changes and updates in local legislations and regulatory guidance.

A summary of roles and responsibilities are set out below:

Role	Responsibilities
Privacy Team	• Co-operates with the business to prioritise the regions for the non-UK/EEA roll-out. • Conducts a gap analysis between EEA/UK data protection laws and the local privacy laws. • Documents the data maps into OneTrust. • Conducting a gap analysis between data maps and the local privacy laws. • Evaluates the existing EEA/UK data protection laws controls to the local privacy requirements. • Approves any requested deviation from the existing EEA/UK data protection law controls. • Supports the local business in implementing the controls.
Business Stakeholders - Business Process Owners and Application Owners	• Assists the Privacy Team in documenting the data maps to OneTrust. • Justifies any necessary deviation from the existing EEA/UK data protection law controls. • Directing the implementation of the necessary controls into processes and assets.
Local Contact Points	• Leads the local privacy project and BAU. • Carries out the implementation and the maintenance of the necessary controls.
Local Law Firms	• Reviews and validates the gap analysis drafted by the Privacy Team.
Compliance	• Detects major changes and updates in local laws and regulatory guidelines and communicates the same to the Privacy Team and other relevant stakeholders.
Regional Head	• Ownership and supervision of the project to ensure the business stakeholders are given the required support to implement the controls.

Below are the local high-level primary privacy and marketing laws applicable to each of Amarillo Brokerage Company's jurisdictions along with information about the relevant statutory regulator.

Brazil

Laws

- The Brazilian General Data Protection Law
- Federal Law no. 12,965/2014 and its regulating Decree no. 8,771/16

The relevant statutory regulator is:

- The National Data Protection Authority

Canada

Laws

- Personal Information Protection and Electronic Documents Act (Likely to be replaced by the CPPA)
- Personal Information Protection Act (Alberta)
- Personal Information Protection and Identity Theft Prevention Act (awaiting to come into force)
- Consumer Privacy Protection Act (under debate)
- Canada's Anti-Spam Legislation

The relevant statutory regulators are:

- Office of the Privacy Commissioner of Canada
- Office of the Information and Privacy Commissioner of Alberta

.

European Economic Area (EEA)

All members of the EEA are subject to the General Data Protection Legislation (GDPR).

- ***France***
    - *Significant domestic law*
        - Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties
        - Decree No. 2019-536
        - French Postal and Electronic Communications Code
    - *Statutory regulator*
        - The Commission Nationale de l'Informatique et des Libertés

- ***Germany***
    - *Significant domestic law*
        - German Federal Data Protection Act
        - German Act Against Unfair Competition
    - *Statutory regulators*
        - Each German state has its own regulator.

- ***Ireland***
    - *Significant domestic law*
        - Irish Data Protection Act 2018
        - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011
    - *Statutory regulator*
        - Data Protection Commission

- ***Netherlands***
    - *Significant domestic law*
        - The Dutch GDPR Implementation Act
        - The Dutch Telecommunications Act
    - *Statutory regulator*
        - The Dutch Data Protection Authority

- ***Norway***
    - *Significant domestic law*
        - Norwegian Personal Data Act
        - Marketing Control Act
        - The Norwegian E-Commerce Act
    - *Statutory regulator*
        - Datatilsynet

Hong Kong

Laws

- The Personal Data (Privacy) Ordinance
- Unsolicited Electronic Messages Ordinance

The relevant statutory regulator is:

- The Office of the Privacy Commissioner for Personal Information

Singapore

Laws

- Personal Data Protection Act of 2012 as amended by the Personal Data Protection (Amendment) Bill
- Spam Control Act

The relevant statutory regulator is:

- The Personal Data Protection Commission

United Kingdom

Laws

- The UK GDPR
- The Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003

The relevant statutory regulator is:

- The Information Commissioner's Office

United States of America

Significant laws

- California Consumer Privacy Act of 2018 soon to be amended by the California Consumer Privacy Rights Act
- CAN-SPAM Act

Significant regulators:

- US Federal Trade Commission
- State regulators