GDPR Policy

The Mexico-UK British Council takes your data protection very seriously. With the introduction of GDPR on 25th May 2018 we have updated our relevant policies and improved our practices and procedures to ensure that any data we hold on our clients is secure. We have also used these regulations as on opportunity look at what data we hold on our clients and delete any unnecessary data.

If you would like to discuss anything in relation to this matter then please contact us at info@mxukbc.org

1. The reasons we collect personal data

We collect and process personal data to:

- Provide business services; representation and lobbying work.
- Market services which may be of interest to you.

2. The lawful bases we rely on to process personal data

We will only use your personal data when the law allows. The law on data protection sets out a number of different reasons (lawful bases) why a company may collect and process personal data. Most commonly, we will use your personal data in the following circumstances.

- In performance of a contract with you. For example, if you take a service from us, we'll collect your contact details in order to deliver the service to you. Where that service is funded by a third party we'll collect information to confirm your eligibility.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, we'll use your contact details to send you direct marketing information telling you about business services that we think might interest you.
- Where we have your consent to do so. For example, when it may be relevant to connect you to other organisations.
- Where there is a legal requirement. For example, to pass on details of people involved in fraud or other criminal activity affecting us to law enforcement.

2a. Third Party service providers

We rely on third-party service providers to perform a variety of business operations on our behalf. In so doing, we may need to share your personal information with them. We provide our service providers with only the personal information they need to perform the services we request and we require that they respect the security of your personal data and to treat it in accordance with the

law. We do not allow our third-party service providers to use your data for their own purposes and only permit them to process your personal data for specific purposes and in accordance with our instructions

Sometimes we will need to share your personal data with third parties and suppliers outside the European Economic Area (EEA). Any transfer of your personal data will follow applicable laws and we will treat the information under the guiding principles of this Privacy Notice.

3. Data retention period

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

4. Data Subjects

You have the right to:

- Request access to the personal data we hold about you, free of charge in most cases.
- Request correction of your personal data when incorrect, out of date or incomplete.
- Request erasure of your personal data.
- Object to processing of your personal data where we are relying on your legitimate interest and there is something about your particular situation, which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- You have the right to request a copy of any information about you that Mexico-UK Business Council/Capstone Allied, S.C. holds at any time, and also to have that information corrected if it is inaccurate.
- You have the right to make a complaint at any time to the National Institute of Transparency, Access to information and Personal Data Protection (INAI), the Mexican supervisory authority for data protection issues www.ifai.org.mx. We would, however, appreciate the chance to address your concerns before you approach the INAI so please contact us in the first instance.

No fee is usually required - You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

If we choose not to action your request we will explain to you the reasons for our refusal.

If you wish to exercise any of the rights set out above, please contact us via email at: info@mxukbc.org

5. How and where is our data stored?

All information is stored on encrypted devices. The data is restricted as to who can access it, and all data is stored on password protected equipment.

Email correspondence and related information is stored in secure servers administered by Google. For more information please visit Google Cloud Security and Compliance Whitepaper

6. Employee awareness

All Mexico-UK Business Council employees have had GDPR awareness training. We constantly review how we collect, control and communicate data. All employees are part of this process. GDPR awareness training is also part of our new employee/associate induction process.

7. Security Data Breach Register

All employees whether temporary or permanent, contractors, third parties and Directors are all responsible for reporting any personal data breach to our Compliance Manager. For any internal data breach considered to be low risk, the breach is notified within 24 hours to our Director of Operations and recorded. We also capture other information in terms steps we will take to limit the damage and steps to reduce risk of reoccurrence. All information will then be recorded on our Data Breach Register.

Where a personal data breach is considered serious and high risk and likely to result in high risk to the rights and freedoms of the data subject, then the relevant supervisory authority is notified within the timescales required by EU legislation.