

Data Protection Policy for International Facilitators Plus UK Ltd.

Introduction

International Facilitators Plus UK Ltd gathers and uses information about individuals. These individuals can include customers, suppliers, business contacts employees and other people the organisation has a relationship with. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Data Protection Law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. Personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The privacy policy of International Facilitators Plus UK, Ltd asserts that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside of the EEA unless that country or territory also ensures an adequate level of protection

Policy Scope

This policy applies to International Facilitators Plus UK, Ltd and to all data that the company holds relating to identifiable individuals. This will include, but not be limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Phone numbers
- Company names and addresses

Responsibilities

Everyone employed by International Facilitators Plus UK, Ltd carries responsibilities for ensuring that data is collected, stored and handled appropriately. Data must be handled in line with this policy and with data protection principles.

The people with key areas of responsibility are:

- The Board of International Facilitators Plus UK, Ltd is ultimately responsible for ensuring that the company meets all of its legal obligations
- The Data Protection Officer, Patricia Hyslop, is responsible for:
 - Keeping the board updates about data protection responsibilities, risks and issues
 - Reviewing all data protection procedures and related policies in line with an agreed schedule
 - Arranging data protection training and advice for the people covered by this policy
 - Handling data protection questions from staff and anyone else covered by this policy
 - Dealing with requests from individuals to see the data International Facilitators Plus UK, Ltd holds about hits, also called subject access requests
 - Reviewing any contracts or agreements with 3rd parties that may handle the companies sensitive data
 - Approving data protection statements attached to emails
- The IT managing company is responsible for:
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
 - Performing regular scans and checks to ensure security hardware and software is functioning properly
 - Evaluating any third-party services the company is considering using to store or process data.

General Staff Guidelines

- Only those requiring access to personal data covered in this policy should have access to it
- Data should not be shared informally. When access to confidential information is required, employees can request it from their Manager
- International Facilitators Plus UK, Ltd will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure by taking sensible precautions following the guidelines below
- Strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people either within the Company or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required it should be deleted and securely disposed of
- Employees should request help from the Data Protection Officer if they are unsure of any aspect of data protection.

Data Storage and Use

For data stored on paper:

- It must be kept in a secure place where unauthorized people cannot see it.
- When not required paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people can see them
- Data printouts should be shredded and disposed of securely when no longer required

For data stored electronically:

- Data should be protected by strong passwords that are changed regularly and never shared
- Data on removable media (i.e. CD or DVD) must be kept locked away securely
- Data should only be stored on designated drives and servers and should only be uploaded to an approved secure cloud server if used
- Servers with personal data should be sited in a secure location away from the general office space
- Data should be backed up frequently, and backups should be tested regularly according to the company's standard backup procedures
- Data should not be saved directly to laptops or other mobile devices such as tablets or smart phones
- All servers and computers containing data should be protected by approved security software.
- When working with personal data, employees should ensure the screens of their computers are locked when unattended
- Personal data should not be sent by email as this is not a secure form of communication
- Personal data should not be transferred outside of the EEA unless that country or territory also ensures an adequate level of protection

Data Accuracy

International Facilitators Plus UK, Ltd will take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of the Company and its employees take reasonable steps to ensure data is accurate and up to date.

- Data should be stored in as few places as necessary. Staff should not create any unnecessary additional data sets
- Staff should take every effort to ensure that data is updated, i.e. confirm a customer details when they call
- Data should be updated as inaccuracies are discovered, i.e. remove a customer from a database when they are not reachable with the current details on file

Subject Access Requests

All individuals who are the subject of personal data held by International Facilitators Plus UK, Ltd are entitled to:

- Ask what information the Company holds about them and why
- Ask how to gain access to it
- Be informed on how to keep it up to date
- Be informed on how the Company is meeting its data protection obligations

These requests are called “subject access requests”. The identity of anyone making a subject access request must be verified before the Company or its employee hands over any information.

Disclosing Data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances International Facilitators Plus, UK Ltd disclose requested data. However the Privacy Officer will ensure that the request is legitimate, seeking assistance from Senior Management and from the Company’s legal advisers.

As part of your enquiry we may collect your name, telephone, mobile and email contact details and information to assess your service requirements.

We may use your email or telephone contact number/s to contact you with regards to your enquiry and subsequent quotation for services if appropriate.

If you are providing information and/or contact data for a third party (i.e. employer) we assume that you have their explicit consent to share this with us. They retain the right to access, correct or remove this information at any point.

How we use and store your personal information.

Data may be stored electronically to communicate with you with regards to your enquiry or for other necessary services. Electronic data will be stored in a secure file location and would be accessible to the service team members and Management of International Facilitators Plus, UK Ltd. Any hard copies of your data will be securely shredded following your enquiry.

Data Breach

In the event of a data breach International Facilitators Plus, UK Ltd will notify those affected within 72 hours while assessing the risks to people’s rights and freedoms. The Company will also, if appropriate, report this breach to the ICO.

How to contact us

Please contact us if you have any questions about our privacy policy or information that we hold about you.

Patricia Hyslop – Data Privacy Officer

By telephone: 02083 265 606

By email: info@ifpglobal.com

By writing: International Facilitators Plus UK Ltd., Great West Business Centre– Suite 18, Great West House, Great West Road, Brentford, TW8 9DF