Privacy Policy

Introduction

Insured Windows Guarantees Ltd (IWG) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations.

This policy sets out the expected behaviours of IWG's Employees, Members and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an IWG Contact.

Personal Data is any information which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. IWG, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements.

Scope

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

Policy

Governance

Data Protection Officer

IWG has established a Data Protection Officer (Susan Oates) whose duties include:

- Informing and advising IWG and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions.
- Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions.
- Acting as a point of contact for and cooperating with Data Protection Authorities
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests.
- Informing senior managers, officers, and directors of IWG of any potential corporate, civil and criminal penalties which may be levied against IWG and/or its Employees for violation of applicable Data Protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
    - provides Personal Data to a IWG Entity
    - receives Personal Data from a IWG Entity
    - has access to Personal Data collected or processed by a IWG Entity.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by IWG in relation to this policy, the Data Protection Officer will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness.
  - Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights.
  - Personal Data transfers.
  - Personal Data incident management.
  - Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The Data Protection Officer, in cooperation with management, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

Data Protection Principles

IWG has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, IWG must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means IWG must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means IWG must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and, kept up to date. This means IWG must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means IWG must,

wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. IWG must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means IWG must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient

Data Subject Consent

IWG will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, IWG is committed to seeking such Consent.

Data Subject Notification

IWG will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures2 will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Protection. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notice

The IWG website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

Data Use

Data Processing

IWG uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of IWG.
- To provide services to IWG customers.
- The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by IWG to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that IWG would then provide their details to Third Parties for marketing purposes.

Data Retention

To ensure fair Processing, Personal Data will not be retained by IWG for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which IWG needs to retain Personal Data is for a period of 10 years + 90 days from the date of completion of any installation.

All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

IWG will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

Data Subject Requests

IWG will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, IWG will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require IWG to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If IWG cannot respond fully to the request within 30 days, the following information will be provided to the Data Subject within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).

- The name and contact information of the IWG individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Law Enforcement requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If IWG Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If IWG receives a request from a court or any regulatory or law enforcement authority for information relating to an IWG Contact, you must immediately notify the Office of Data Protection who will provide comprehensive guidance and assistance.

Data Protection Training

All IWG Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, IWG will provide regular Data Protection training and procedural guidance for their staff.

Data Transfer

IWG may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

Policy Maintenance

The Data Protection Officer is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to IWG Employees.