Live-in Guardians

DATA AND PRIVACY

POLICY STATEMENT

Live-in Guardians General Data Protection Regulations (GDPR) Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Scope:

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Who is covered under the General Data Protection (GDPR) Policy?

Employees of our company must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements:

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time, agreed with client and employees
- Transferred to organizations, countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information

- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Card Payments over the phone

- Check amount to be paid by the customer and key in details directly to the card machine
- Email or post customers copy of receipt directly to the customer
- File merchant copy receipts for 12 months in a secure facility and then shred in a cross shredder.

Accuracy

Live-in Guardians will take reasonable steps to keep personal data up to date and accurate.

Personal data will be stored for 6 years after an employee has worked for the organisation and brief details for longer. Unless the organisation is specifically asked by an individual to destroy their details it will normally keep them on file for future reference. The Managing Director has responsibility for authorising the destruction of personnel files.

Storage

Personal data that is kept in paper-based format is held in a secure cabinet and electronically on a password-protected computer system.

Every effort is made to ensure that paper-based data is stored in organised and secure systems.

Live-in Guardians operate a clear desk policy at all times.

E-mail

Live-in Guardians will send emails for the purposes of marketing, recipients will have to have double subscribed to this service and Live-in Guardians will retain history of the recipient's agreement to be contacted with marketing materials. Relevant emails will then be sent to the recipient for a fixed period of time before engaging the recipient to re-subscribe to the service. An unsubscribe procedure is in place at all times.

Live-in Guardians will also send emails to customers without permission however these emails will only be transactional, for example when a customer buys a service through one of Live-in Guardians websites, order confirmation, delivery of service information and invoices will be sent to recipients via email.

Use of Photographs

Where practicable, Live-in Guardians will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website or in the Newsletter.

External data records

Purposes

Live-in Guardians obtains personal data (such as names, addresses, card payments and phone numbers) from Clients, Suppliers, Contractors / interested parties. This data is obtained, stored and processed solely to assist staff in the efficient running of services. Personal details supplied are only used to send material that is potentially useful. Most of this information is stored on the organisation's database.

Live-in Guardians obtain personal data and information from clients and members in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by the client/ member.

Consent

Personal data is collected in person, over the phone and using other methods such as e-mail.

Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation, in which case HR or a member of Management Team will discuss and agree disclosure with the Managing or Operations Directors.

Access

Only the organisation's staff will normally have access to personal data.

All staff are made aware of the General Data Protection Regulations Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service.

Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g. the Inland Revenue.

Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made.

All confidential post must be opened by the addressee only.

Compliance

Compliance with the (GDPR) is the responsibility of all staff, paid or unpaid. Live-in Guardians will regard any unlawful breach of any provision of the Act by any staff, paid or unpaid, as a serious matter which will result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

Retention of Data

No documents will be stored for longer than is necessary.
Any data stored indefinitely will be in a secure environment be it electronic or paper.

All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

If data is maintained this will be held securely

Actions:

To exercise data protection, we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- No use of unauthorised software
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks using up to date Cyber essentials or Anti-Virus software.

- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

Disclosure Barring Service (DBS) (Where applicable)

Live-in Guardians will act in accordance with the DBS's code of practice.

Copies of disclosures are kept for no longer than is required. In most cases this is no longer than 6 months in accordance with the DBS Code of Practice. There may be circumstance where it is deemed appropriate to exceed this limit e.g. in the case of disputes.

Responsibilities of Employees

During the course of their duties with Live-in Guardians, where staff will be dealing with information such as names/addresses/phone numbers/e-mail addresses, card payments of other staff and clients.
They may be told or overhear sensitive information while working for the company. The General Data Protection Regulations (GDPR) gives specific guidance on how this information should be dealt with. In short to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Staff, paid or unpaid must abide by this policy.

To help staff meet the terms of the General Data Protection Regulations (GDPR); the attached Data Protection/Confidentiality statement has been produced. Staff are asked to read and sign this statement to say that they have understood their responsibilities as part of the induction programme.

Disciplinary Consequences:

All principles described in this policy must be strictly followed.

A breach of data protection guidelines will invoke disciplinary and possibly legal action.

This policy applies to all those employed by Live-in Guardians.

Date: 28th May 2018

Signed: Arthur Duke

Managing Director

ICO Guidance

The ICO have compiled a data protection reform website to help organisations understand and adapt to the General Data Protection Regulation (GDPR). Visit the data protection reform website here.

A checklist is also provided with 12 steps to take now in preparation for the GDPR. Download "Preparing for the General Data Protection Regulation (GDPR)" here.