LegacyForesight

Privacy Notice

August 2018

Introduction

The General Data Protection Regulation (GDPR) is European wide data protection legislation that requires organisations working with individuals based in the European Economic Area to meet certain requirements regarding the collection, processing, security and destruction of personal information.

As we undertake research that collects or evaluates personal information about a living person who can be identified from the information they have provided we aim to ensure compliance with the General Data Protection Regulation.

Legacy Foresight Limited is registered with the UK Information Commissioners Office as a Market Research/ Research Organisation with the registration reference ZA145723.

Purpose

This policy sets out how Legacy Foresight and its Associates will seek to ensure compliance with the legislation.

Application

This policy applies to Legacy Foresight's dealings with respondents, clients and third parties that may be involved in processing 'personal information'. It covers the way personal information will be obtained, used, shared, physically stored and destroyed.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) governs the **processing** (i.e. obtaining, holding, organising, recording, retrieval, use, disclosure, transmission, combination and destruction) **of personal and sensitive data** (i.e. information relating to a living individual - the data subject) and sets out the rights of individuals whose information is processed in manual

or electronic form or held in a structured filing system. There are six principles that describe the legal obligations of organisations that handle personal information about individuals. These Principles are:

1. *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individual.*

The information we gather about an individual will be collected in a way where they are fully informed how we intend to use that information, for what purposes and how we will share it.

2. *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.*

We will explain why we need the information we are collecting and not use it other than for those purposes.

3. *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

We will only collect the information we need to provide the services required.

4. *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

The information we collect will be accurate and where necessary kept up to date. Inaccurate information will be removed or rectified as we become aware of the changes.

5. *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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals*.

We will not hold information for longer than is necessary.

6. *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, using appropriate technical or organisational measures*.

We will make sure that the personal information we hold is held securely to ensure that it does not become inadvertently available to other organisations or individuals.

Legacy Foresight fully supports these principles.

Handling personal information, lawfully, fairly and transparently

The first and second principles require Legacy Foresight to acquire and process personal information lawfully, fairly and in a transparent way. Legacy Foresight therefore is clear at the outset about the purpose for which information is obtained and processed. Legacy Foresight aims to ensure that:

1. respondents and potential respondents are aware of the purpose or purposes for which the information is to be used and they have a choice as to whether to provide the information;
2. a respondent is able to ask for confirmation of the source of their personal information;
3. personal information is not used in ways that would have adverse effects on individuals;
4. respondents are provided with easy to read and understand informed consent sheets when information is collected;
5. personal information will only be handled in ways that individuals would reasonably expect;
6. the third-party providers we work with to provide potential respondents must comply with the requirements of the General Data Protection Regulation as well;
7. marketing undertaken by us will be undertaken in a manner that complies with the General Data Protection Regulation;
8. we seek to uphold the individual's rights with regard to their personal information.

Appropriate records will be maintained to demonstrate compliance with the above-mentioned requirements.

Data security

Legacy Foresight has appropriate security measures to prevent personal information held being accidentally or deliberately compromised. In particular, Legacy Foresight:

- is clear about everyone's responsibility for ensuring information security;
- makes sure that the correct physical and technical security is in place, backed up by robust processes and procedures and reliable, well-trained staff; and
- is ready to respond to any breach of security swiftly and effectively.

Legacy Foresight recognises that information security breaches may cause real harm and distress to the individuals if their personal information is lost or abused (this is sometimes linked to identity fraud).

Computer equipment, security and updates

We are aware of the vulnerability of laptops, phones and removable media and the business owners takes steps to ensure the security of these devices.

We ensure that all equipment used as part of our business processes is appropriately protected and secured. The equipment we use has up to date Malware and anti-virus software. When updates are notified because of a software patch, these are applied as they become available.

The laptops that are used for business purposes are password protected to ensure that any personal information contained within them is appropriately secured.

Outsourcing

Legacy Foresight has procedures in place if we use third parties to process information to ensure that we:

- only choose a data processor that provides sufficient guarantees about its security measures to protect the information and the processing it will carry out;
- take reasonable steps to check that those security measures are working effectively in practice; and
- put in place a written contract setting out what the data processor is allowed to do with the personal information or business information.
- notify any data controllers with whom we are working, who the proposed data processor will be.

Legacy Foresight requires third parties that it works with to ensure that there are adequate security measures in place to secure the information that is being held.

Data loss

If personal information is accidentally lost, altered or destroyed, attempts to recover it will be made promptly to prevent any damage or distress to the individuals concerned. In this regard Legacy Foresight considers the following:

- containment and recovery – the response to the incident includes a recovery plan and, where necessary, procedures for damage limitation.
- assessing the risks – assess any risks and adverse consequences associated with the breach, as these are likely to affect how the breach needs to be contained.
- notification of breaches – informing the Information Commissioner's Office or other relevant Supervising Authority as necessary (within 72 hours), law enforcement agencies, data controllers on whose behalf we are working and individuals (whose personal information is affected) about the security breach is an important part of managing the incident.
- evaluation and response – it is important to investigate the causes of the breach, as well as, the effectiveness of controls to prevent future occurrence of similar incidents.
- additionally, Legacy Foresight would also look to ensure that any weaknesses highlighted by the information breach are rectified as soon as possible to prevent a recurrence of the incident.

Data retention

To comply with information retention best practice, Legacy Foresight establishes standard retention periods for different categories of information, keeping in mind any professional rules or regulatory requirements that apply and ensuring that those retention periods are being applied in practice. Any personal information that is no longer required will either be archived or deleted in a secure manner.

Legacy Foresight's retention periods for different categories of personal information are based on individual business needs and contractual obligations.

Legacy Foresight understands the difference between permanently deleting a record and archiving it. If a record is archived or stored offline, it will reduce its availability and the risk of misuse or mistake. If it is appropriate to delete a record from a live system, Legacy Foresight will also delete the record from any back-up of the information on that system, unless there are business reasons to retain back-ups or compensating controls in place.

Destruction of Electronic Records

All electronic files are destroyed by deletion and then the use of an electronic file shredder. This ensures that all electronic information is deleted permanently and cannot be recovered.

Secure disposal of records and computer equipment

Once the retention period expires or, if appropriate, the customer or business information is no longer required; paper records should be disposed of in a secure manner. All paper records containing customer or business information are disposed of by shredding. This includes all archived records.

All used computers, printers and any other electronic equipment that may contain or that will have stored customer or corporate information in electronic format must be disposed of in an appropriate manner after the information has been completely wiped off. An external provider will be used to ensure that the memory on the devices is completely clean of information before the item is disposed of.

Training

Legacy Foresight takes its responsibilities with regards to ensuring training is undertaken seriously. We know that having policies and procedures in place provides a solid base for our training programme and we aim to undertake training in accordance with the role and seek specialist advice as and when required. All training is documented and reviewed regularly.

Data Protection Officer

Legacy Foresight does not at this time meet the requirements for a dedicated Data Protection Officer but this is kept under review as the type of work and range of clients/respondent's changes. We are committed to meeting the needs of the General Data Protection Regulation and if our business requires a DPO, we will seek to appoint one.

Review

This policy will be reviewed periodically considering changing business priorities and practices and to consider any changes in legislation.