Mary Kerin

Data Protection and Security Policy

June 2018

Contents

Introduction

The General Data Protection Regulation 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.

Purpose

This policy sets out how Mary Kerin will seek to ensure compliance with the legislation.

Application

This policy applies to Mary Kerin's dealings with clients and third parties that may be involved in processing customer related information. It covers the way personal information should 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.

Mary Kerin fully supports these principles.

Handling personal information, lawfully, fairly and transparently

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

1. there are comprehensive marketing plans and operational procedures in place for initiating contact with prospects and generating sales in a manner that complies with the General Data Protection Regulation;
2. personal information is collected and used only when there are legitimate business reasons which are balanced against the interests of the individual concerned;
3. personal information is not used in ways that would have adverse effects on individuals;
4. the purpose or purposes for which the information is to be used is made clear to individuals and they have a choice as to whether to provide the information.
5. Individuals are provided with easy to read and understand privacy notices when information is collected;
6. personal information will only be handled in ways that individuals would reasonably expect; and
7. on request, we can provide to the individual a copy of the personal information we hold about them.

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

Consent

Consent will be required for certain types of information usage, generally relating to mailing lists and marketing communications.

When consent is required, it must be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms, and be in clear and plain language. The individuals consent to using their personal data must be as easy to withdraw as to give. Consent must be "explicit" for sensitive data. Mary Kerin is required to be able to demonstrate that consent was given.

Under the Privacy and Electronic Communication Regulations (PECR) there are specific requirements relating to unsolicited direct marketing communications. A solicited communication is one that is actively invited, either directly by the customer or via a third party. An unsolicited communication is one that the customer has not invited but they have indicated that they do not, for the time being,

object to receiving it. If challenged, businesses would need to demonstrate that an individual has positively opted in to receiving further information from us.

Mary Kerin understands that it is unlawful to contact customers or organisations that have informed us that they do not wish to receive unsolicited marketing material. Therefore, Mary Kerin are aware of and comply with the following:

Telesales – Mary Kerin ensure that individuals and organisations they wish to contact are not registered on the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS) respectively. If they are registered or have directly notified Mary Kerin not to call, then unsolicited direct marketing calls will not be made to them.

Faxes – similarly individuals and organisations that have registered with the Fax Preference Service ("FPS") or have directly notified Mary Kerin not to contact them by fax, will not be sent unsolicited direct marketing faxes.

Emails and text message – Mary Kerin will not contact individuals by email or via text message without obtaining prior consent unless the individual's details have been obtained in the course of a sale or negotiations of a sale. Individuals will be given the opportunity to opt out of receiving further marketing emails or texts each time that such contact is made.

The Mailing Preference Service (MPS) is managed by the Direct Marketing Association and supported by Royal Mail to enable individuals to register their names and addresses to limit the amount of direct mail they receive. Unsolicited marketing material will not be sent by post to individuals that have informed Mary Kerin they do not wish to receive such information or they have registered with the MPS.

Mary Kerin maintains internal logs of individuals and organisations that have indicated that they do not wish to receive unsolicited marketing information and conduct checks against the TPS, CTPS, FPS, eMPS and MPS databases as appropriate.

When data is purchased from third parties for prospecting purposes, Mary Kerin ensures that the data has been acquired by the third party through fair and lawful means, the data can be used for the purposes of unsolicited marketing activities and that the data has been cross-checked by the third party against the appropriate preference service databases.

PECR and cookies

Under the PECR, as from 26 May 2011, businesses must seek consent before any cookie is set on an individual's computer.

Cookies are small, often encrypted text files, located in browser directories. They are used by companies to help users navigate websites efficiently and perform certain functions. Cookies are also used to keep computer users logged in and their personal details private or for tracking their activity so that companies can improve the website. Cookies can be used by third parties to track information about individuals and spam them with adverts. By themselves, cookies pose no risk since they do not contain viruses.

Session cookies enable the website to track user movement from page to page so that the user does not get asked for the same information again. The most common example of this functionality is the shopping cart feature of an e-commerce website. Session cookies are never written on the hard

drive and they do not collect any information from the user's computer. Session cookies expire at the end of the user's browser session.

Persistent cookies are stored on the user's computer and are not deleted when the browser is closed. Such cookies can retain user identities and preferences, allowing those preferences to be used in future browsing sessions.

Mary Kerin is responsible for ensuring that the websites comply with the PECR and that, where necessary, appropriate information is disclosed to website users and consent is obtained from users before cookies are set.

Fair treatment

Fairness generally requires us to be transparent, i.e. clear at outset and open with individuals about why the information is being collected and how it will be used. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

Mary Kerin aims to ensure that, in all cases, consent and privacy statements will:

- be clear, fair and not misleading;
- explain the consequences of not providing the required information;
- explain how long the information will be kept for;
- explain if the replies to questions are mandatory or voluntary;
- explain if the information will be transferred overseas;
- explain that if the information will be shared, who with and how they will use it;
- explain how customers may be contacted e.g. telephone, email, SMS, post;
- explain customers' rights – e.g. they can obtain a copy of their personal information;
- explain who to contact if they wish to know more information about how their information is held or to opt-out of receiving further information or if they need to complain; and
- explain customers' right to complain to the Information Commissioner's Office.

Mary Kerin is responsible for ensuring that the following details are communicated to clients:

1. the identity of the business or if appropriate, its nominated representative;
2. the purpose(s) for which the business intends to process the prospect's or customer's personal information and if the information is to be shared or disclosed to other organisations (so that the individual concerned can choose whether or not to enter into a relationship with the company sharing it);
3. any additional information that will enable the business to process the information fairly; and
4. how customers can access the information held about them (as this may help them to spot inaccuracies or omissions in their records – see section below on Rights of Data Subjects).

Minimum amount of personal data

Under the principles of GDPR, Mary Kerin identifies the minimum amount of personal data we need so as to properly fulfil our purpose. We ensure that we hold that much information, but nothing further. If we need to hold particular information about certain individuals, we only collect the information for those individuals and nothing more. Mary Kerin does not hold personal data on the off-chance that it might be useful in the future.

Accurate and kept up-to-date

Mary Kerin will:

- take reasonable steps to ensure the accuracy of any personal information they obtain;
- ensure that the source of any personal information is clear;
- Establish if the individual has challenged the accuracy of the information, this is evaluated and recorded carefully; and
- consider whether it is necessary to update the information, particularly if the purpose relies on the information being current.

Mary Kerin understands that an expression of an opinion about an individual is classed as their personal information. The record of an opinion (or of the context it is held in) will contain enough information to enable a reader to interpret it correctly. If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, Mary Kerin understands that it is even more important to state the circumstances or the evidence it is based on. Any remarks made in emails or system notes would need to be disclosed if the individual. Therefore, Mary Kerin ensures that records do not contain anything that might be considered derogatory, or offensive, even though the record is generally for internal use.

Rights of Individuals

The General Data Protection Regulation creates specific rights of individuals. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Subject Access Requests

An individual has the right to see the information that Mary Kerin holds about them and can make a request to access this information. Requests must be responded to within 30 days of receipt.

In line with the GDPR, Mary Kerin will request certain information before responding to a request:

- enough information to judge whether the person making the request is the individual to whom the personal information relates to avoid personal information about one individual being sent to another, accidentally or as a result of deception.
- Sufficient information that would reasonably be required to find the personal information amongst the records held by the company and covered by the request.

In the event of an individual making a subject access request via a third party Mary Kerin will request written consent from the individual to confirm that the third party can request and receive information on the individual's behalf.

An individual who makes a request is entitled to be:

- told whether any personal information is held and being used;
- given a description of the personal information, the reasons it is being processed, and whether it will be shared with any other organisations or individuals;
- given a copy of the information; and
- given details of the source of the information (where this is available).

Requests for information from law enforcement agencies

The General Data Protection Regulation includes exemptions, which allow personal information to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the information, and regardless of the purpose for which the information was originally gathered. Mary Keri will release personal information to law enforcement agencies if required to do so.

Shared Documents

Mary Kerin has shared cloud access provided to those we work with to support the use and transmission of documents and information. To ensure effective security protocols, when accessing documents on the shared drive, they should be downloaded to a computer to be worked on or reviewed and then uploaded when changes have been completed or the documents have been viewed.

Access to the shared drive is set up to automatically disconnect after a period of inactivity.

Data security

Mary Kerin has appropriate security measures to prevent personal information held being accidentally or deliberately compromised. In particular, Mary Kerin

- have designed and organised security to fit the nature of the personal information held and the harm that may result from a security breach;
- are clear about everyone's responsibility for ensuring information security;
- make sure that the correct physical and technical security is in place, backed up by robust processes and procedures and reliable, well-trained staff; and
- are ready to respond to any breach of security swiftly and effectively.

Mary Kerin 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).

Managing and monitoring staff

Mary Kerin ensures that staff or those acting on their behalf are aware of, trained and comply with regulatory requirements and company policies on data protection and information security matters.

There are controls in place to ensure that those people handling customer or confidential business information are honest and trustworthy and do not disclose information about customers without checking the identity of callers and verifying that they are entitled to the information being requested.

There are controls in place to ensure that only authorised personnel can access, alter, disclose or destroy personal information and only act within the scope of their authority. All paper records containing customer information and commercially sensitive information are stored securely when not in use and desks are cleared at the end of the working day.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was put together by the PCI Security Standards Council to decrease payment card fraud across the internet and increase credit card data security. Mary Kerin complies with the PCI-DSS requirements, this is enforced by the 'acquiring bank' through whom we have our merchant account.
There are twelve key requirements for organisations:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for passwords or other security parameters.

3. Protect stored data.
4. Encrypt the transmission of cardholder data and sensitive information.
5. Use and regularly update anti-virus software.
6. Develop and maintain securer systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Outsourcing

Mary Kerin 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.

Mary Kerin 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.

Restrictions on transferring information to non EEA countries

There are no restrictions on moving personal information within EEA countries. As Mary Kerin uses cloud services, we know that personal information will be held within the EEA. We are open and transparent with our clients and potential clients about where their information is processed and accessed.

Mary Kerin considers the following factors when deciding whether or not to transfer information overseas:

- the nature of the personal information being transferred;
- how the information will be used and for how long; and
- the laws and practices of the country where information is being transferred to.

We also consider additional factors such as:

- the extent to which the country has adopted data protection standards in its law;
- whether there is a way to make sure the standards are achieved in practice; and
- whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

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 Mary Kerin 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 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, Mary Kerin 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, Mary Kerin 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.

Mary Kerin's retention periods for different categories of personal information are based on individual business needs.

Mary Kerin 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, Mary Kerin 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.

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, fax machines, 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.

Monitoring & Reporting

The Operation Director will monitor the adherence to this policy and report to the other directors any issues or concerns regarding its compliance.

Review

This policy will be reviewed periodically in light of changing business priorities and practices and to take into account any changes in legislation.