# Merlinco Ltd

## Data Protection and Security Policy

**Updated May 2018**

## Contents

## 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 Merlinco Ltd undertake survey research data processing that can include 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.

## Purpose

Our policy shows how Merlinco Ltd will seek to ensure compliance with the legislation. This is in addition to our compliance with the Market Research Society's Code of Conduct, which provides assurances to respondents in terms of anonymity in data processing for analysis - https://www.mrs.org.uk/standards/code_of_conduct

## Application

This policy applies to Merlinco Ltd'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, processed, 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 process about an individual will be collected in a way where respondents are fully informed about how that information will be used, 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.* If we collect the data then we will explain why we need the information we are collecting and not use it other than for those purposes. If our client collects the data then we will seek assurances that GDRP compliant consent has been given and recorded.

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 and process the information we need to provide the services required. If we are supplied with personal data but do not need

it for the purposes of the survey data processing then we shall not retain that part of the survey data records.

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 and/or process will be accurate and where necessary kept up to date. Inaccurate information in respect of personal data will be removed or rectified as soon as we become aware of any 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 to provide data processing services – typically this will be one year.

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.

Merlinco Ltd fully supports these principles.

## 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.

## Handling personal information, lawfully, fairly and transparently

The first and second principles require Merlinco Ltd to acquire and process personal information lawfully, fairly and in a transparent way. Merlinco Ltd therefore is clear at the outset about the purpose for which information is obtained and processed. Merlinco Ltd 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 understand privacy notices 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. we seek to uphold the individual's rights with regard to their personal information.

## Consent for survey respondents – and use of data

As the lawful basis for processing survey research data, respondent consent will be required. It must be freely given, specific, informed and unambiguous. Requests for consent will be separate from other terms, and be in clear and plain language. The individual's consent will be "explicit" where it relates to sensitive data. Merlinco Ltd is required to be able to demonstrate that respondent consent was given. We therefore maintain records of client's consent to meet the accountability requirements for both the profession and the requirements of the General Data Protection Regulation. Merlinco Ltd will only process personal data for which respondent consent has been given, and will not use the information for any purpose other than anonymous survey analysis.

## Computer Equipment, Security and updates

We are aware of the vulnerability of laptops, phones and removable media and the business owners take steps to ensure the security of these devices, including the use of encryption and password protecting any files containing personal data.

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 encrypted and password protected to ensure that any personal information contained within them is appropriately secured.

It is not our practice to use unsecured phones for business purposes. If a phone is used for personal information then two factor authentication is applied to the handset.

## Removable Media

Any removable media used such as an external hard drive or USB pen drive are encrypted.

## 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.

## Minimum amount of personal data

Under the principles of GDPR, Merlinco Ltd identify the minimum amount of personal data we need 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 and/or process that

information for those individuals and nothing more. Merlinco Ltd does not hold personal data on the off-chance that it might be useful in the future.

## Accurate and kept up-to-date

Merlinco Ltd will:

- take reasonable steps to ensure the accuracy of any personal information they obtain;
- ensure that the source of any personal information is clear;
- consider whether it is necessary to update the information, particularly if the purpose relies on the information being current.

## Subject Access Requests

An individual has the right to see the information that Merlinco Ltd holds about them and can make a request to access this information. Requests must be responded to within 30 days of receipt. Such requests may come from individuals directly if we have collected the data, or through our clients. In line with the GDPR, Merlinco Ltd 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.

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. Merlinco Ltd will release personal information to law enforcement agencies if required to do so.

## Data security

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

- 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.

## Outsourcing

Merlinco Ltd have 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.

Merlinco Ltd 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, but personal data must not be transferred or processed outside of that geographical area.

## 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 Merlinco Ltd consider 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, Merlinco Ltd 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, Merlinco Ltd establish 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 deleted in a secure manner.

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

Merlinco Ltd 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 shall be disposed of in a secure manner. All paper records containing customer or business information are disposed of by shredding or returned to the client.

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.

## Training

Merlinco Ltd undertakes to provide GDPR training for all staff who have access to personal data, in accordance with their role, and seek specialist advice as and when required. All training is documented and reviewed regularly.

## Data Protection Officer

Merlinco Ltd has appointed John Tebboth as a Data Protection Officer, responsible for all aspects of GDPR compliance. Any questions about Merlinco's GDPR policy, implementation, security or possible access by individuals should be addressed to John Tebboth at Merlinco Ltd.

## Review

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