Data protection and Handling Policy 2018

Introduction

At Treemonkey our business is to carry out research into people and their families for the purpose of genealogy and to build up a family history. This process involves obtaining, collating, interpreting and storing personal information. To carry out this research we have to use some personal information and share it purely for the purpose of genealogy and family history research

We care very deeply about the security of the personal information we hold and as such carry out regular data protection training enabling us to comply with legislation. We are registered with the Information Commissioners Office (ICO) registration number A8226454. The ICO is the UK's Supervisory Authority. They make sure everyone follows the rules to keep personal data safe. They give advice and also deal with complaints about data being used wrongly - if they feel that concerns are justified, their job is then to investigate and take action. If a data breach occurs, it's the ICO they'll need to report to, and if someone in your organisation fails to comply with the regulations in any way, it's the ICO our organisation will answer to.

Statutory Regulations

The *General Data Protection Regulations 2018* (GDPR) and supersedes the *Data Protection Act 1998*. It covers personal data about an identifiable, living person. It can be anything from a name, a photo, an email address, a person's bank details, posts on social media, medical information, details about work performance, subscriptions, purchases, tax number, education, location, username and password, hobbies, habits, lifestyle, or even computer IP addresses. This is not an exhaustive list.
It is also data that could reasonably be put together with other information to find something out about a person, or information that could make it possible for a person to be uniquely singled out in a group of people.

Some personal data is considered to be more sensitive than others – the GDPR calls these '*special categories of personal data*'. They include data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership. Special categories also include genetic data, biometrics and data concerning health, sex life, including sexual orientation and data related to criminal convictions, offences and related security measures

Other types of information that the GDPR considers to be more sensitive includes financial data and data which could lead to discrimination. It also includes data which is protected by a legal or professional secrecy obligation and data that could be misused for identity fraud.

And data about children under the age of 16 requires special protection, as they are particularly vulnerable and may not understand the risks involved in giving out their personal data.

The GDPR protects all **personal** data from **anything** we are likely to do with it, making sure it's only used in the way the person whose data it is has agreed to.

The Rights of our Customers

One of the most important aspects of the GDPR is that it gives a person certain rights over the personal data that's held about them. These rights are at the heart of data protection, along with the principles of data protection.

Every one of our customers has:

The right to be informed

We will be fair and transparent information on everything we intend to do with the data. The data will only be used for genealogy and family history research. Our policy is to keep as little paper based information as possible. Where documents are provided/loaned to us we generally scan them into an electronic archive where they are processed and stored then return the originals. We will keep personal data for 24 months from the last communication we had from our customer unless the customer has requested in writing that we keep it longer. After this time has elapsed we will destroy the data and it will not be able to be retrieved.
We do have to share data with other database holders and researchers purely for genealogy and family history research
If at any time a customer requests that data is changed or deleted the request must be made in writing. We will carry out the request within 28 days.
We will not make any automated decisions based on the data we hold
Customers have the right to withdraw consent for us to carry out research and /or hold data.
Customers have the right to complain to the ICO if they believe a data breach has occurred
Customers have the right to be told this information at the time the data is obtained.

The right of access

We will at any time provide upon request, supply details of the personal information we hold about our customers in a clear and intelligible form and, if it's known, any information about where it came from. We will also confirm that their data is being, or has been processed, where this happened and what it has been used for and if

the information was used to make a decision about them, along with the logic involved in making that decision.
If a customer wants to know what information our organisation has about them, then they write to us and ask for a copy. This is called a **"**Subject Access Request**"**

The request has to be a written request, but it can be written on paper, emailed or faxed.
It will be provided free of charge in an electronic format. We are then legally required to provide that information, within one month of receiving the request. We will do this if we have received the request in writing and we are satisfied that the customer is who they say they are.

The right to rectification

Customers can, on request, have any mistakes corrected in the data held about them, We will respond to these requests within 1 month (or 2 months if it's particularly complex). This helps ensure that data is accurate.
If the personal data in question has been disclosed to third parties, the third parties must be informed of the rectification too - where possible. Customers must also be informed about the third parties to whom the data has been disclosed, where appropriate.

The right to erasure, also known as the right to be forgotten

Customers have the right to have all the data we hold on them deleted. Some of the reasons for erasure include: if holding their data is no longer necessary, if it's no longer relevant to the original purposes of processing, if they withdraw their consent, or if their data was processed unlawfully.

The right to restrict processing

Customers have the right to prevent us from processing their data any further. We can store it, but not process it any more. We will keep hold of just enough information on the customer to make sure their restriction is respected in the future.

The right to data portability

Customers may ask your us to provide them with their data - to be used however they like across different services, for example they could move it to another organisation, or they may ask us to directly transfer it. We will provide them with a machine readable, structured, electronic copy of all their data usually in GEDCOM format.

The right to object

Customers have the right to object to direct marketing to stop their information being used to sell them things – for example by email or cold calling; or to object to the processing of their personal data for scientific or historical research and

statistics; or to object to the processing of their data based on legitimate interests or the performance of a task in the public interest, or exercise of official authority (including profiling)
We will not use personal information for reasons other than genealogy and family history research within the scope already agreed with the customer.

Rights in relation to automated decision-making and profiling

We will not use the personal data we have to carry out automated decision-making and profiling. Any such activity if used will always be with the prior consent of the customer and will always be backed up by manual human verification

Our Data Protection Mission Statement

1: Lawfulness, fairness and transparency

Everything we do with personal data, from collecting it and holding it, to retrieving, organising and destroying it, will be done lawfully, fairly and in a transparent manner.

2: Purpose Limitation

We will only use the personal information we have for the purpose previously agreed with our customer.

3: Data Minimisation

We will only ask for information which is relevant to the reason you're collecting it.

We will not ask for information simply because it might be useful in the future. Information should be on a **need to know** basis and we will explain why we are asking for it.

We will carry out regular reviews, looking at the data we have and check it's still necessary to complete their intended purpose.

4: Accuracy

Reasonable steps be taken to ensure the accuracy of any data we obtain. Where any errors in data are identified, we will take all reasonable steps to rectify the problem and let you know what we are doing and why.

Data protection and Handling Policy 2018

5: Storage Limitations

We will only keep personal data for as long as it's needed. So, when data is no longer needed for the purpose it was collected, it will be deleted.

We will let customers know before deleting any information

6: Integrity and Confidentiality

We will take all reasonable steps to ensure customers personal data is safe and secure (protecting data from accidental or deliberate loss, destruction, damage or unauthorised access). Most of our records are kept electronically. The following steps are used, but not limited to:

- Using a Firewall, virus-checking software, anti-malware and anti-spyware software, strong passwords
- Backing-up data
- Restricting access to authorised persons only
- Disposing of computers – properly removing all personal data first
- Shred paper documents before disposing of them

7. Accountability

We have an internal set of policies and procedures to ensure that personal data is kept secure. These are checked on a regular basis to ensure they are suitable and sufficient