

Data protection policy

Last updated: April 2022

1 Introduction

This document sets out Elegant Words' policy on the protection of the personal data of all business contacts – primarily customers (actual and potential), other people involved in projects that I work on (such as authors and typesetters), service/product providers (actual and potential), individuals who may be mentioned in projects that I work on, and fellow editors and proofreaders.

It is intended to ensure compliance with the General Data Protection Regulation (GDPR – see definition below), which became effective on 25 May 2018, and was retained in UK law as of 1 January 2021 despite the UK's exit from the European Union.

2 GDPR roles

I am both the Data Controller and the Data Processor for Elegant Words.

I am a sole trader, running my business and providing my services alone. There is no requirement for a Data Protection Officer to be appointed for a business of this type and size.

3 Types of data

As part of the running of my business, I obtain contact details of individuals (clients, service providers etc., as stated in Section 1). These individuals may be acting alone or as part of an organisation.

These details are primarily email addresses, telephone numbers and postal addresses, but could also include Skype IDs and other contact details. My understanding is that these details may be considered to be within the scope of the GDPR *if, and only if* they can be used to identify *named individuals*.

For the purposes of this policy, contact details that can be identified only with *organisations*, or with *groups etc.* within organisations (for example, a company office address or group email address), are assumed to be outside the GDPR's scope.

I do not actively collect or store 'sensitive personal data' as defined in the GDPR, such as ethnic origin or religious or political beliefs. If such data is contained within a document that I am asked to work on:

- I will not use or share this data in any way, other than sharing the document, as necessary, with other parties who are involved in the project;
- I usually delete the document (and certainly if requested to do so by the client or Data Subject), after the invoice for work has been paid by the client.

4 Collecting data

4.1 Postal addresses

To comply with HMRC's requirements, I need to obtain a postal address for each client that I work for, to be included in invoices that I issue.

For my future reference, I may store this postal address in a list of client details on my computer(s) *if* it relates to an organisation, or a group etc. within an organisation, but not if it is an individual's address. In either case, I may include it in the contacts list in an email account, if I think I might need it for a potential future invoice.

4.2 Email addresses

As part of normal email correspondence, email addresses are automatically recorded in the email accounts that I use.

However, I do not store these addresses in a separate file, unless they are *group* email addresses that I may need to refer to – for example, the address of an accounts team that I should send invoices to. In these cases, I may store them in my list of client details on my computer(s).

When researching potential clients, service providers etc., I may store individuals' *company-based* email addresses in spreadsheets if, and only if, I have obtained them from publicly available sources (such as a company website). I will not do this for email addresses associated with private individuals.

My website does not have a login system for visitors. I do not collect email addresses via my website.

I do not use mailing lists.

4.3 Other personal data

As part of normal communication, individuals' telephone numbers may be stored (automatically or manually) in the contacts list on my mobile or landline telephone.

5 Use of data

I believe that my use of the above data is compliant with the GDPR, as I simply use it for contacting people about work and related matters, and (as per Section 4) to include postal addresses in invoices. In GDPR terms, I believe these to be 'lawful bases' for use of the data.

6 Security of data

The data referred to in the above sections is stored on the computer(s) that I use for my work.

I have a single computer that I use for my regular, everyday work. It requires a password on start-up and on wake-up. I do not use a laptop or tablet or any other device for my work.

I use full-disc encryption such that all files are encrypted.

All medicolegal reports I work on for expert witnesses are either password-protected or I use an encrypted email client.

The operating system I use is Windows 10's latest supported version with regular security updates and full anti-virus software.

I store nothing in the cloud.

My email accounts are password-protected, and my mobile telephone requires a PIN on start-up and wake-up.

7 Retention of data

All documents containing confidential information, particularly medical and medicolegal reports, are deleted once the client has paid the invoice relating to that document.

As required by HMRC, I retain each postal address (at least in invoices, and sometimes also in my spreadsheet of client details, as per Section 4.1) for at least six years from the date when I last used it. After that, I will delete it on request from the client, or may delete it as part of a 'housekeeping' exercise.

8 Website

My website, <https://www.elegantwords.co.uk/> does not need a cookie policy because it does not store or retrieve any information from a computer that accesses it. The website uses HTTPS security.

I sometimes use systems such as Google Analytics to assess how web users have generally been finding and navigating my website; however, I do not use them to identify individual visitors.

9 Sharing of data with third parties

I will not share personal data with any other parties without the Data Subject's consent, unless it needs to be shared with HMRC for tax audit purposes.

10 Consent and awareness

As I do not process personal data for any purposes other than those described in Section 5, I do not believe that any of my data processing activities require consent from my clients or other contacts, or from any Data Subjects.

However, as part of the process of agreeing work, I will provide the client with a copy of, or a link to, this policy, unless (a) they have already been made aware of it, and (b) in the meantime, in my judgement, the policy has not been changed in any way that affects that client.

I do not believe that, in normal circumstances, there is a requirement for other types of contacts (service providers, fellow editors, etc.) to be prompted to read this policy.

If someone sends me an electronic document containing contact details, I will not be obliged to delete the document or redact those details, as they will have been supplied to me voluntarily. However, I will delete the document or redact details on request from the document provider or Data Subject, unless this would prevent me satisfying any legal requirements.

11 Rights of Data Subjects

I acknowledge and will respect the rights afforded to Data Subjects under the GDPR, including the rights:

- to be told, on request, what data I hold about them
- to ask for data to be updated, deleted, restricted or moved to another party without hindrance, subject to my legal requirements
- to complain to the Information Commissioner's Office about any alleged misuse of data.

Following any request to update, delete, restrict or move data, I will give an initial response within 15 days if at all possible, and (if it is to go ahead) carry out the requested action within 30 days. If necessary, I will delete relevant emails as well as deleting data from files.

12 Responding to data breaches

If I become aware of a possible breach of data protection within my business, I will investigate it as soon as possible. If I find that a breach has occurred and could result in a risk to anyone's privacy rights or freedoms, I will report it to the Information Commissioner's Office within 72 hours of determining this.