Data protection policy

Last updated: 23 January 2020, 11:21 AM BST

1 Introduction

This document sets out GH Editorial's 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) 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.

2 Definitions

Data Subject – The individual who the data in question relates to, and who may be identified by that data.

GDPR – The European Union's General Data Protection Regulation.

HMRC – The UK's tax regulator.

I, *my*, etc. – Graham Hughes, trading as GH Editorial, of Chester, United Kingdom.

Organisation – This includes both commercial businesses and not-for-profit organisations.

A glossary of GDPR terms can be found here.

3 GDPR roles

I am both the Data Controller and the Data Processor for GH Editorial.

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.

4 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 will delete the document if requested to do so by the client or Data Subject, after the work is completed.

5 Collecting data

5.1 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.

5.2 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, other than those that are automatically added to a list when visitors comment on blog posts and specify their email addresses (which is optional). My website hosting system, Weebly, collects these without my involvement – I do not process this data or store it elsewhere.

I do not use mailing lists.

5.3 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.

A number that is stored on my mobile telephone might be automatically synchronised into the contacts list in an email account that I use. I also might add it to one of these contacts lists manually, if I think this will help me to contact the person.

When I make contact with people via Skype, their Skype IDs are automatically visible to me within Skype itself, as normal. I do not normally store them elsewhere, but might do so with the Data Subject's consent.

6 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 5.1) to include postal addresses in invoices. In GDPR terms, I believe these to be 'lawful bases' for use of the data.

7 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 primary computer that I use for my regular, everyday work. I also have a laptop and tablet, for contingency purposes and occasional out-of-office use. Each of these devices requires a password or PIN on start-up and on wake-up.

The data referred to in the above sections is normally stored on my primary computer only. I may occasionally transfer it temporarily between the above devices, via either (a) a reputable, secure, cloud-based system such as Google Drive, Microsoft OneDrive or Dropbox, or (b) an external hard drive or flash drive, which I will not share with any third party. This might be to enable short-term out-of-office working or a migration to a new primary computer. I will only hold it in this temporary storage for as long as is necessary for the relevant purpose

(for a migration to a new computer, this will include a short ‘settling in’ period, typically a few weeks, in case problems arise with that computer).

The data is backed up using a reputable system (currently Norton Security), which imposes password protection on the backup files. This will allow me to recover reasonably up-to-date versions of files onto another device if my primary computer breaks down. The data is not stored on any other backup storage, either online or offline, other than in the temporary circumstances described in the previous paragraph.

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

8 Retention of data

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 5.1) 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.

9 Website

My website, www.gh-ed.com, has a cookie policy, which covers the collecting of cookies when visitors browse the site. The website uses HTTPS security. It is hosted by Weebly, whose approach to GDPR protection is documented here.

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.

10 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.

11 Consent and awareness

As I do not process personal data for any purposes other than those described in Section 6, 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.

(Before 25 May 2018, I invited some existing clients, whom I considered to be active clients, to read this policy.)

I will not advise *past, inactive* clients about this policy, unless they offer me further work.

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 (for example, the joining instructions for a training course), 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.

For organisational clients, the policy may be reviewed by either (a) one of my primary contacts in the organisation, or (b) another person in a suitable position of authority.

12 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.

13 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.

Update history

Version	*Date*	*Summary of changes*
1.1	9 May 2018	Removed letterhead. In Section 1 (‘Introduction’): included ‘other people involved in projects that I work on (such as authors and typesetters)’ as potential business contacts. Clarification in Section 5.2 (‘Email addresses’): ‘I will not do this for email addresses associated with private individuals.’ Change in Section 7 (‘Security of data’): my computer requires a password on wake-up, as well as on start-up. Expansion of Section 9 (‘Website’, formerly ‘Website analytics’) to cover website privacy and security as well as use of analytics tools; and to mention analytics tools in general, not just Google Analytics. Changes in Section 11 (‘Consent and awareness’, formerly ‘Consent’), after further consideration: it no longer specifies that clients must state their acceptance of this policy – I will simply ask them to read it.
1.2	8 June 2018	In Section 9, the privacy policy (for my website) is now called the ‘cookie policy’, with a different link. Also adjusted wording to reflect this.
1.3	18 Dec 2018	Amended and expanded Section 7 (‘Security of data’) to cater for the possible use of additional computers, describing how and when data may occasionally be transferred between them. Changed ‘computer’ to ‘computer(s)’ in some sections, in line with the above. Updated some references to the introduction of the GDPR on 25 May 2018, to reflect the fact that this is in the past.
1.4	23 Jan 2020	Amended Section 7 (‘Security of data’) to include flash drives as well as external hard drives. Amended Section 11 (‘Consent and awareness’) to remove the requirement to ask a client to read this policy. Instead, I will just make them aware of it.