Bryce Editorial Services

Data Protection Policy

1 Introduction

This documents sets out Bryce Editorial Services' data protection policy in order to comply with the General Data Protection Regulation (GDPR) coming into effect on 25 May 2018. It explains how I use and store the personal data of all business contacts, be they client (actual or potential), other people I collaborate with on projects (such as authors), service/product providers (actual or potential) and fellow editorial professionals (this includes students enrolled on proofreading and copy-editing courses).

2 GDPR roles

I'm a sole trader, which means that I'm running my business and provide all its associated services by myself. As such, I'm both the data controller and data processor for Bryce Editorial Services. There is no requirement for me to appoint a data protection officer for this kind and size of business.

3 Types of data

As part of the day-to-day running of my business I obtain contact details of individuals (i.e. those named in the introduction); these individuals (also referred to as 'data objects' in the context of the GDPR) may be acting alone or on behalf of an organisation. These details include primarily email addresses, but can also include postal addresses, telephone numbers and Skype IDs, but need not be limited to these in individual circumstances. It is my understanding that these details may be considered to come under the scope of the GDPR if they can be used to identify named individuals; contact details that identify only organisations, or certain groups within organisations, are considered to be outside the scope of the GDPR.

I don't collect or store any 'sensitive personal data' as defined by the GDPR, i.e. information concerning a data object's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health, sex life or sexual orientation, or details of criminal offences. In the unlikely event that such information is contained in a document I'm asked to work on, I will:

- not share or use this data in any way other than, if required, sharing it with other parties involved in the project
- delete the document if requested to do so by the individual in question after the work is completed.

4 Collecting data

4.1 Email addresses

Email addresses are automatically recorded in Microsoft Outlook (or BT Mail in my capacity as online course tutor) as part of normal email correspondence; however, I remove these where they can identify an individual every so often as part of general housekeeping or when I haven't heard from the person in question for a year. Students' email addresses and any email correspondence are deleted once a student's access to the course has expired, which is usually after six months.

I don’t store these addresses on a separate file unless they form part of an invoice, in which case the invoice is stored in electronic form in a folder for the relevant tax year, and for a period of five years on hardcopy after the 31 January submission deadline for the relevant tax year in order to comply with Her Majesty’s Revenue and Customs (HMRC) requirements.

My website doesn’t have a login system for visitors and I don’t collect email addresses via my website; where a potential client leaves their email address on the contact form, this is voluntarily given, and storage applies as it does to all other email addresses, as outlined above.

I don’t use mailing lists.

4.2 Postal addresses

To comply with HMRC’s requirements I need to obtain a postal address for every client I work for, to be included on invoices that I issue. I keep address details for both organisations, or groups within organisations, and individuals on file on my computer for future reference for the duration of the tax year to which they refer, and then for five years on hardcopy after the 31 January submission deadline for tax purposes, as outlined in section 4.1 above.

4.3 Other personal data

As part of normal business other personal data such as telephone numbers or Skype IDs may be stored in email form, by the person supplying the relevant information, in a folder with the organisation’s/individual’s name in Microsoft Outlook for the duration of the project and for six months after publication of the title/document in case of queries, after which all email correspondence relating to the project will be deleted.

5 Use of data

I believe that the use of the above-mentioned data is compliant with the GDPR as I use it only for the purposes of contacting people about work and related matters and to include postal addresses on invoices. In GDPR terms I believe these to be ‘lawful uses’ for the use of the data.

6 Security of data

The data referred to in the sections above is stored on the computer I use for work; it requires a password on start-up and wake-up. The data that I keep in files on the computer is backed up using an external hard drive that, although not password protected, is stored in a secure location in my office at home. I don’t use cloud storage to back up personal data.

Both of my email accounts are password protected. Occasionally I may have reason to access my work emails from either my mobile phone or my tablet computer; my mobile requires the user to input the correct pattern and my tablet is password protected.

7 Retention of data

As outlined in sections 4.1 and 4.2 above, I retain addresses (both email and postal) on invoices for five years after the 31 January submission deadline for the relevant tax year, as required by HMRC. I will destroy the hardcopies after that period.

8 Website

My website, http://bryceeditorial.co.uk, does not use cookies, and I don’t use services such as Google Analytics.

9 Sharing of data with third parties

I will never share personal data with a third party without the consent of the individual in question, unless it is required for HMRC tax audit purposes.

10 Consent and awareness

As I don't process personal data for any purposes other than those described in section 5, I believe that none of my data processing activities require the consent from the individuals concerned, be they clients or other contacts. However, from 25 May 2018, as part of the process of agreeing to work, I will provide the client (existing or new) with a link to, or copy of, this policy, asking them to read it, unless (a) they have already been prompted to read it, and (b) in the meantime, in my judgement, the policy hasn't changed in any way that affects the client.

I will not advise past clients, whom I consider to be inactive, about this policy, unless they offer me further work.

I don't believe that under normal circumstances there is a requirement for me provide other types of contact (e.g. service providers, fellow professionals) with a link to, or copy of, 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 the individual in question, unless this would prevent me from satisfying any legal requirements.

For organisational clients, this policy may be reviewed by either one of my primary contacts in the organisation or another person in the organisation with suitable 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
- ask for data to be updated, deleted, restricted, or moved to another party without hindrance, subject to my legal requirements
- 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

In the event of my becoming 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 I will report it to the Information Commissioner's Office within 72 hours of determining this.

Drafted 23/05/2018