INDEPENDENT BOOKSELLERS FORUM

Guides to Practical Bookselling

General Data Protection Regulation (GDPR)

Frequently Asked Questions

Table of Contents

General

Q: I know I have to produce some new documentation to be GDPR compliant (privacy notice, data inventory, subject access request procedure, etc). Can the BA just produce some model documentation for me?

A: Unfortunately, as the new documentation (privacy notice, data inventory, subject access request procedure, etc) needs to be bespoke to each business and as the BA isn't a legal advisor, we aren't able to produce model templates. We can, however, point people towards the key information to include in these documents as listed on the ICO website (eg privacy notice, data inventory).

Q: Is there just one document I should read, to tell me what I need to do to comply with the GDPR?

A: The Information Commissioner's Office (ICO) have produced this 12 step guide for businesses, which is what we're recommending booksellers work through. Some of the steps may not be particularly relevant to your business, and others may be relevant but may not take very long to implement to make sure you're compliant.

The ICO also have an overview of the General Data Protection Regulation here, which we recommend you read as an overview.

Q: Have the Information Commissioner's Office (ICO) produced any material for small and medium businesses?

A: The Small and Micro business advice from the ICO can be found here, including some FAQs for retailers and a small businesses helpline. We recommend reading through this advice and the FAQs, so you're familiar with the background and the resources they have available.

Q: Can I speak to anyone at the BA if I have questions which aren't covered in this document?

A: Yes. Please call 0207 421 4640 and ask to speak to Pippa Halpin for GDPR guidance. Please note that the BA cannot provide legal advice, just practical guidance.

Working with other businesses

Q: Who is the data controller for data stored on Bertline and Gardlink?

A: Bertrams and Gardners have confirmed that the bookseller is the data controller for all personal data stored on their systems.

Q: Will Bertrams' and Gardners' systems be GDPR compliant?

A: Yes, they have teams of people working on ensuring compliance. They will be in communications with their customers regarding GDPR compliance and about how they will work with booksellers to be compliant in time for 25th May 2018.

Q: Will Mailchimp be GDPR compliant?

A: The BA understands that Mailchimp are fully compliant with the GDPR: click here to view the document they have circulated to explain how they comply.

Q: What steps do I need to take to make sure I'm using Mailchimp in a way that's compliant with the GDPR?

A: Click here to see how to create Mailchimp sign-up forms which are GDPR compliant.

Please see the 'Marketing' section in this document for other steps you may need to take.

Q: Who is the data controller for data stored on TicketSource?

A: TicketSource have confirmed that the bookseller is the data controller for all personal data stored on their systems.

Q: What steps do I need to take to make sure I'm using TicketSource in a way that's compliant with the GDPR?

A: Click here for information about how to use TicketSource's new GDPR-compliant system features, including their guidance on obtaining granular marketing consent and adding your Privacy Notice to the online booking process.

Working with customer orders

Q: What should I do with my receipts?

A: Most receipts don't contain personal data and so don't fall under the scope of the GDPR.

If your receipts contain personal data, then you shouldn't keep them for longer than is necessary and you should dispose of the data securely (by shredding).

Q: What should I do with customer/school invoices?

A: See here for details about how long to store financial records. The GDPR says you should store personal data 'for as long as necessary', so you are fine to keep invoices until you are no longer legally required to keep them. You should then dispose of them securely (by shredding or digital deletion).

Q: When a customer/school places an order with us, we take a note of the customer's name, e-mail and phone number to let them know when it has arrived. Should we be adding a tick box on the form to indicate that the customer agrees to us holding their details for that one occasion?

A: The legal basis for processing personal data in this instance is 'necessary for performance of a contract' rather than 'consent'.

So you don't need a tick box in this instance: in fact, the ICO recommend that you shouldn't ask for consent in such instances, as it can be misleading/unfair, as the legal basis for processing their personal data in this instance isn't 'consent'.

You can keep the personal data relating to the order for as long as is necessary (for example, until the required years have passed for financial purposes, or until you have contacted the customer to let them know their order is in) and then it should be securely deleted/destroyed (by shredding or digital deletion).

What you *should* do is create a Data Inventory (an Excel spreadsheet) which will list all the types of personal data you hold, what you do with it, and your legal basis for doing it. This is a step towards complying with the GDPR 'accountability' requirement. The Data Inventory should include:

- A list of the types of personal data you hold (eg names, email addresses, postal addresses for staff, customers, suppliers)
- How you obtained this information (eg face to face, by email, via a paper form, through social media)
- Where you store this information (eg in a physical file, on your computer, in the cloud, on a wholesaler's database)

- Who you share this information with (eg no-one, wholesalers, other local businesses, suppliers)
- How long you store this information for before deleting it (eg a month, a year, seven years)
- The legal basis you are relying upon for each instance of processing the personal data (eg consent, necessary for performance of a contract, etc)

If you then plan to use the personal data for marketing purposes, then that's a different situation (see the 'Marketing' section).

Q: Is a customer's order history 'personal data' or even 'sensitive personal data'? If so, do we need explicit consent before taking an order?

A: No. The ICO have confirmed with the BA that you can't identify someone's sensitive personal data based just on their order history. For example, a customer might buy eight books on Jewish history for their dissertation, or because they themselves are Jewish: there is no way to tell just from the purchase history which of those is the case. So the ICO confirmed that the content of the purchases itself cannot count as personal data, as without additional evidence (for example, a customer saying that they are Jewish), it is impossible to definitively identify additional personal data from their purchases.

If they just tell you verbally some sensitive personal data (a.k.a. 'special categories of data'), that doesn't count as formal 'processing' either as you are not writing anything down, so you don't need explicit consent for this either.

However, if a customer verbally shares some sensitive personal data (a.k.a. 'special categories of data'), for example the fact that they are transgender, and then you log this in writing in some way (because, for example, they may have asked you to source particular books on that area), then that particular piece of information is definitely sensitive personal data (a.k.a. a 'special category of data') and should be treated accordingly. Here's a link to how to treat sensitive data a.k.a. 'special categories of data'.

Working with regular customer subscriptions

Q: I provide monthly book subscriptions to customers. We need to hold the recipients' data for long periods - an annual subscription typically. The subscriptions are bought online, by phone and in the shop. Do I need to get the customer's consent to use their data every time I send them a book?

A: No. For paid subscriptions, technically your 'legal basis' for processing the data is actually 'necessary for performance of a contract' rather than 'consent'. Please click here to see the different legal bases.

This means that you don't need to ask for consent to process the personal data in this instance: in fact, the ICO recommend that you shouldn't ask for consent in such instances, as it can be misleading/unfair, as the legal basis for processing their personal data in this instance isn't 'consent'.

You can keep the data for as long as is necessary: presumably until the annual subscription has been fulfilled, and then possibly a couple of months afterwards in case they wish to renew. Then it should be securely deleted/destroyed (by shredding or digital deletion).

When the annual subscription has expired, you should still be able to contact the customer (even though technically your 'contract' with them has expired) to ask them if they would like to renew, based on the legal basis of 'legitimate interest'.

This legal basis only applies to customers who have an existing relationship with you and so would *reasonably expect* to be contacted by you again, even if their subscription has ended. It would be less likely to apply if they hadn't had a subscription with you for, say, five years and you sent them an email asking them if they'd like to re-join the subscription scheme.

What you *should* do is create a Data Inventory (an Excel spreadsheet) which will list all the types of personal data you hold, what you do with it, and your legal basis for doing it. This is a step towards complying with the GDPR 'accountability' requirement. The Data Inventory should include:

- A list of the types of personal data you hold (eg names, email addresses, postal addresses for staff, customers, suppliers)
- How you obtained this information (eg face to face, by email, via a paper form, through social media)
- Where you store this information (eg in a physical file, on your computer, in the cloud, on a wholesaler's database)
- Who you share this information with (eg no-one, wholesalers, other local businesses, suppliers)
- How long you store this information for before deleting it (eg a month, a year, seven years)
- The legal basis you are relying upon for each instance of processing the personal data (eg consent, necessary for performance of a contract, etc)

If you then plan to use the personal data for marketing purposes, then that's a different situation (see the 'Marketing' section).

Q: What about for gift subscriptions, for example where a customer buys a gift subscription for a friend and gives us their friend's home address for the postal delivery (i.e. personal data is provided by one person about another person)? Do I need to get the gift recipient's consent?

A: No. The ICO have confirmed with the BA that you can make strong arguments for relying on either the 'necessary for performance of a contract' legal basis or the 'legitimate interest' basis in this instance, rather than 'consent'. They said it's completely up to you which you decide to choose, but that you should carefully record your reasons either way, so you can demonstrate your arguments in case a customer ever complained.

1. Choosing to rely on 'Necessary for performance of a contract': they said that this could be appropriate as arguably you would need to process the gift recipient's data in order to fulfil your side of the contract with the purchaser.

2. Choosing to rely on 'Legitimate interest': the ICO said that although you could make a strong argument for relying on the 'necessary for performance of a contract' legal basis, they thought that possibly in this instance, relying on the 'legitimate interest' basis would be a better option.

   They said that the situation is unlikely to infringe on any rights of the recipient. They also said that although you haven't had prior contact with the gift recipient, you could strongly argue that they should *reasonably expect* to be contacted by a business who has been contracted by a friend/relative to contact them. The ICO said that the recipient can *reasonably expect* an organisation to fulfil their contract in this way and that therefore you can make a strong argument for this being a lawful legal basis.

If you decide that 'legitimate interest' is likely to be the best legal basis, you'll need to record your reasons for this, as well as taking into account these other considerations.

In either case, you don't need to include an opt-out option with each gift, as the legal basis for processing their personal data is not 'consent'.

Marketing

Q: Can I use the details of current/previous customers for marketing purposes?

A: Very possibly.

You could make strong arguments for relying on either the 'consent' legal basis or the 'legitimate interest' basis (if you've already been contacting them for marketing purposes and they could *reasonably expect* to keep receiving emails from you).

The ICO say it's completely up to you which you decide to choose, but that you should carefully record your reasons either way in your Data Inventory, so you can demonstrate your arguments in case a customer ever complained. You should also make sure that customers can easily opt-out of receiving your marketing messages.

a. Choosing to rely on 'consent':

Recital 42 of the GDPR says: 'Where processing is based on the data subject's consent, the controller should be able to *demonstrate* that the data subject has given consent to the processing operation.'

It also has to be '*opt-in, clear and granular'*. Your mailing list may already be compliant with this if customers have *opted-in* positively to subscribe to your one specific emailing list.

However, unfortunately if you don't have *evidence* that these subscribers 'opted-in' positively in response to clear and granular consent options (which possibly you may not), then you are supposed to get fresh, GDPR-compliant, consent.

Many small businesses are sending out simple emails to their mailing list to ask them to quickly reconfirm their consent (see the following example). Please click here to see the requirements for fresh valid consent. Mailchimp are doing a good job at supporting customers in this way so do check with them to see what they have in place.

Dear Manny,

You're receiving this email because you have previously signed up to the Black Books mailing list.

This means you're always one of the first people to hear about our latest offers, author events, community events and competitions. But changes in data protection law mean **we need you to confirm that you're still happy for us to stay in touch**.

Click on the button below to confirm your email subscription. If you don't, we won't be able to send you future updates on Black Books' events and offers.

Yes, I'd like Black Books to stay in touch by email

Thanks for your support,

Bernard Black

b. Choosing to rely on 'Legitimate interest':

The ICO have said that if you have already been in contact with a consumer via marketing email, the recipient can *reasonably expect* an organisation to contact them in this way and that therefore you can make a strong argument for this being a lawful legal basis.

If you decide that 'legitimate interest' is likely to be the best legal basis, you'll need to record your reasons for this, as well as taking into account these other considerations.

Q: Can I use the details of new potential customers for marketing purposes?

A: For any customers or potential customers that you add to your marketing list in the future, your legal basis would probably need to be 'consent' as they won't have a pre-existing relationship with you and wouldn't *reasonably expect* to be contacted by you without agreeing to this.

You would need to make sure you comply with the GDPR standards for consent.

Working with previous customers

Q: We have many dormant customers on our database who may have a single invoice record from, say, 2014. We know we have to keep this for financial purposes, but do we need to get consent from our dormant customers to hold their data for financial reasons?

A: The legal basis for processing personal data in this instance is/was 'necessary for performance of a contract' rather than 'consent'.

So you don't need to have consent from the customer in this instance: in fact, the ICO recommends that you shouldn't ask for consent in such instances, as it can be misleading/unfair, as the legal basis for processing their personal data in this instance isn't 'consent'. This means you don't need to contact your customers to check that you can still hold their data for financial reasons.

You can keep the personal data relating to the invoice for as long as is necessary (for example, until the required years have passed for financial purposes) and then it should be securely deleted/destroyed (by shredding or digital deletion).

If there is personal data attached the dormant customer which is not necessary to be kept for financial purposes (eg their email address), then you should have a time scale (often called a 'Retention Schedule') for going through and deleting this data after a particular point in time. The GDPR states you can keep this data 'as long as is necessary for the purposes of processing': this is quite vague, so you can decide a sensible period. Perhaps if they haven't been invoiced for, say, three years, you will decide to delete this additional personal data.

What you *should* do is create a Data Inventory (an Excel spreadsheet) which will list all the types of personal data you hold, how long you hold it for, and your legal basis for keeping/using it. This is a step towards complying with the GDPR 'accountability' requirement. The Data Inventory should include:

- A list of the types of personal data you hold (eg names, email addresses, postal addresses for staff, customers, suppliers)
- How you obtained this information (eg face to face, by email, via a paper form, through social media)
- Where you store this information (eg in a physical file, on your computer, in the cloud, on a wholesaler's database)
- Who you share this information with (eg no-one, wholesalers, other local businesses, suppliers)
- How long you store this information for before deleting it (eg a month, a year, seven years)
- The legal basis you are relying upon for each instance of processing the personal data (eg consent, necessary for performance of a contract, etc)

Working with pre-owned stock

Q: As a used book seller we often find names, addresses or emails inscribed into books and text books. Do we need to marker out all names etc inscribed into books?

A: The ICO told the BA that this was the safest option. If the person is living and identifiable, and there isn't a lawful basis for processing it, then you should delete it – work through the lawful bases just to double check. Possibly 'legitimate interest' may apply, but if you can't find a legal basis then unfortunately you will need to delete the data securely.

Q: If so does that apply to antique books as well?

A: If the personal data belongs to a deceased individual, GDPR doesn't apply.

Q: As a used book seller, we often find invoices, letters, photos, etc hidden away in used books. We already put shred the invoices: should we be doing the same with letters or photos? Sometimes these can be very old.

A: If you're not holding onto the letters or photos, then yes, you should shred them.

If you're looking to hold onto the letters or photos, then:

a) If the owner is dead, GDPR doesn't apply, so you're fine.

b) If the owner may still be alive, you need to identify a legal basis for processing. Possibly 'legitimate interest' may apply, but if you can't find a legal basis then unfortunately you will need to dispose of the data securely.

Use of the ICO material