GDPR and Cyber Security – BA member communications

Bookselling Essentials

June 2017 Pg 12
Be Cyber Aware and Alert!

Since last summer, the BA Council has been looking at Cyber Security. BA executives have met representatives from GCHQ, the National Cyber Security Centre, and from the Office for Security and Counter-terrorism at the Home Office, to determine what practical steps members might take to protect their data from those with malevolent intent.

We have worked with specialist advisers to produce a simple check list for our SME members. Here are our 12 suggestions:

Check list for small and medium sized retailers

1. **Install the latest software and app updates.** They contain vital security upgrades which help protect against viruses and hackers.
2. **Run Windows Update.**
3. If you are using Microsoft software, it is important that you apply all Microsoft patches and updates and that you **only use supported Microsoft operating systems to limit your own vulnerabilities. XP and Vista are no longer supported.**
4. **Use proper anti-virus software services.**
5. Make sure your anti-virus product is up to date and **run a scan.**
6. **Use strong and separate passwords for your key accounts,** including email and online banking. Use three random words to make a strong and memorable password.
7. **Never disclose security details** such as passwords or PINs.
8. **Back up essential data** at regular intervals. You can't be held to ransom for data you hold somewhere else.
9. **Just because someone knows your basic details, it doesn't mean they are genuine. If there is something you are not sure about - do not open it.** Please look at the address that is purporting to send you the e-mail. If it reads (for example) something like: From: Tim Godfray (igor@spammer.ru) then it may not be from me! Be careful with emails including links. Our advice would be to go directly to a website rather than click on a link.
10. Provide staff with access to **simple, freely-available cyber security training**.
11. Conduct a **cyber security risk assessment** for your business.
12. Seek accreditation through the Government-endorsed '*Cyber Essentials'* scheme.

Further information
www.cyberaware.gov.uk/toolkit
www.cyperaware.gov.uk/protect-your-business
https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance
www.takefive-stopfraud.org.uk

June 2017 Pg 12
National Book Tokens - Gift Card Security

Cyber security and fraud remain high on the agenda for most businesses; here are a few considerations when dealing with gift cards – please share this information with all store staff.

1) Always use an authorised **real-time** transaction system when redeeming a gift card.

2) When selling, take payment before loading the gift card with value.

3) If you think that an old or vulnerable customer is buying an unusually large value of gift cards you should feel free to ask them why (victim assisted crimes can be avoided by retailer vigilance).

4) When selling larger values of gift card, unless you know the customer, do not accept uncleared cheques or credit/debit cards not supported by PINs.

5) Never let anyone (including NBT staff) know your PIN or passwords for the NBT transaction systems.

6) NBT employees and NBT service providers will never ask you to load cards over the phone as part of a test.

PLEASE NOTE: As far as we are aware there have **not** been any recent fraud attempts either buying or redeeming NBTs and the above advice is simply to support you in maintaining general security levels.

September 2017 Pg 14

Be Cyber Aware and Alert!

Cyber security: a risk booksellers can't afford to ignore

Cyber crime and fraud are major security priorities for all businesses, large and small, and booksellers are no exception. Whether you hold customer's personal details, are processing transactions online, or store valuable data such as an inventory or orders on your devices, you have something of value to cyber criminals, who can use this information to hold your business to ransom, steal money, or commit identity fraud. Yet research from the government's Cyber Aware campaign, in conjunction with KPMG, shows that one in seven businesses in the retail industry do not take steps to protect their data. But this is not an issue booksellers can afford to ignore.

The fall out from a cyber attack can not only be financial, but also reputational. According to the research, 58% of customers said they would be deterred from using a business affected by a cyber attack. While retailers definitely recognise the importance of their customers – 73% of retailers said they place their most value in them – not implementing secure online behaviours puts this crucial relationship at risk.

Fortunately, there are a number of proactive measures businesses can take to mitigate these risks, according to the Cyber Aware campaign. As a first step, businesses need to adopt a cyber security strategy. According to research by Cyber Aware and KPMG, 95% of retailers consider this to be very or quite important to their business, but only 45% of retailers have a formal cyber security plan in place.

The good news is, putting this plan in place is simple and affordable. The Cyber Aware campaign recommends that booksellers take the following measures to protect their businesses, and in turn their customers:

- **Use a strong, separate password for your email accounts** - Having strong, separate passwords for your most important business email accounts means that if hackers steal your password for one of your less important accounts, they can't use it to access your most important ones.
- **Install the latest software and app updates** - They contain vital security updates which help protect your business devices from viruses and hackers. Security updates are designed to fix weaknesses in software and apps which could be used by hackers to attack your devices.
- **Always back-up your most important data** - Safeguard the data most important to your business, such as your inventory, orders or financial information, by backing it up to an external hard drive or a cloud-based storage system. If your devices are infected by a virus or accessed by a hacker, your data may be damaged, deleted or held to ransom by ransomware.
- **Secure tablets or smartphones with a screen lock** – If you use devices such as tablets or smartphones in store to process sales, give these devices an extra layer of security by setting it to lock when you aren't using them. Each time you want to unlock your devices, you will need to enter a PIN, pattern, password or fingerprint. This makes it harder for someone who gets hold of your device to access the data held within it.

Putting these measures in place, and following the latest advice is critical for booksellers. It's an investment worth making - for minimal time and effort now, you can protect your business's data, reputation, and bottom line later.

For further information about the campaign and the free ways Cyber Aware can support you in promoting these messages to your staff and customers (whether it's through social media posts, leaflets or posters) – visit https://www.cyberaware.gov.uk/ [1] Cyber Aware/KPMG Small Business Reputation & The Cyber Risk report (2016)

[1] Cyber Aware/KPMG Small Business Reputation & The Cyber Risk report (2016)

September 2017 Pg 14

BA GDPR guide

Familiar with the Data Protection Act 1998? On 25th May 2018, the EU is introducing a new data protection regulation: the General Data Protection Regulation (GDPR). The UK government has confirmed that Brexit will not affect this: UK companies will still need to comply with the GDPR or face heavy fines.

The BA has produced a brief guide designed to give booksellers an overview of the requirements of the GDPR and to give some practical tips on how to meet these requirements. Some of the requirements are very similar to those of the Data Protection Act 1998, some are more thorough enhancements and some are completely new.

A copy of the guide is available on the BA website, under IBF Practical Guides to Bookselling. Alternatively, email pippa.halpin@booksellers.org.uk to request a copy.

March 2018 Pg 17

General Data Protection Regulation (GDPR) update

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security. There are some heavy fines for non-compliance and small and medium businesses are being warned not to ignore it.

It will affect areas such as: the way customers sign up and unsubscribe to your newsletters, your website set-up, how you store customer details, the way you interact with children online (via Facebook, Twitter, etc) and staff training.

Key changes include:

- an 'accountability' requirement (e.g. you will probably need to create some additional policies and procedures to *show* how you comply)
- a requirement to document your legal basis for processing (e.g. you will need to create a spreadsheet listing all the ways you collect, store and use personal data, and then explain which of the six GDPR 'legal bases' you are relying on for each instance of processing)
- consent must be verifiable, clear and affirmative (e.g. you will probably need to change the wording and processes for signing customers up to your mailing lists)
- additional rights for data subjects (e.g. you will need to update your website privacy notice to list all of your customers' rights, amongst other things; you will need to have a procedure for when an individual requests to view all the personal data you hold about them - i.e. a Subject Access Request; you will need to ensure that the personal data you hold can be easily transferred from one IT environment to another)
- new rules if you use children's personal data (e.g. if you offer online services to children, you may need to get parental consent; you will need to update your privacy notice so a child can understand it)
- breach reporting (e.g. you need to know how and when to report data breaches – for example, if your database is compromised and your customer personal data is destroyed or stolen)

The key place to go for more information is the Information Commissioner's Office (ICO) website www.ico.org.uk. The ICO have many helpful GDPR resources for small and medium businesses, including a new advice service helpline, checklists and steps to take now.

The BA have also produced a short GDPR guide for booksellers which can be found at www.booksellers.org.uk/jointheba/ourservices/IBFguides. To provide further support, we have started sending out GDPR top tips in our bi-weekly enewsletter: this will continue until the end of May 2018.

The BA is not placed to provide legal advice but for more guidance on the GDPR, contact Pippa Halpin 020 7421 4695 pippa.halpin@booksellers.org.uk or make an appointment to see Pippa at London Book Fair 2018 at the **BA Stand 4A41** from 10-12 April.

June 2018 Pg 15

General Data Protection Regulation (GDPR) – what next?

The EU's General Data Protection Regulation (GDPR) came into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security.

So what now? Can businesses forget all about the GDPR, given the deadline for compliance has passed?

Even if you are confident that your business is completely compliant with the GDPR right now, in a year's time you may be using personal data for a new purpose, or you may be collecting different personal data, or you may have a new procedure for handling and storing the personal data. So you should set up regular annual reviews now, to ensure that you continue to comply with the regulation.

If you have any questions about the GDPR or want a copy of our GDPR FAQs document, email pippa.halpin@booksellers.org.uk.

BA Group E-newsletter

16th January 2018

Data Protection - GDPR roundup for BA members

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security.

There are some heavy fines for non-compliance and small and medium businesses are being warned not to ignore it.

It will affect areas such as: the way customers sign up and unsubscribe to your newsletters, your website set-up, how you store customer details, the way you interact with children online (via Facebook, Twitter, etc) and staff training.

The key place to go for more information is the Information Commissioner's Office (ICO) website www.ico.org.uk. The ICO have many helpful GDPR resources for small and medium businesses, including a new advice service helpline. Click here for their GDPR guides, checklists and steps to take now.

The BA has also produced a short GDPR guide for booksellers which can be found here. To provide further support, we will be sending out GDPR top tips in this enewsletter, until the end of May 2018.

If you have any questions about the GDPR, do contact Pippa Halpin 020 7421 4695 pippa.halpin@booksellers.org.uk

General Data Protection Regulation (GDPR) Top Tip

Top Tip: Make sure all decision makers and staff in your shop are aware that the Data Protection law is changing to the GDPR on 25th May 2018. They need to appreciate the impact this is likely to have.

This might involve:

- Reading through the guides on the ICO (Information Commissioner's Office) website www.ico.org.uk to make sure you know what things might need to change in the way you run your business/the way you manage your shop.
- Making sure the owners know they will need to create some additional policies and documentation.
- Making sure the owners know they may need to add the GDPR to their budget and company risk register.
- Setting aside a regular slot of time each week to work through the ICO's checklists (with other key decision makers, if relevant).
- Organising a staff meeting with shopfloor booksellers to highlight some of the key changes they need to know about.
- Setting a date for some refresher data protection training for your staff.

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security. There are some heavy fines for non-compliance and small and medium businesses are being warned not to ignore it.

If you have any questions about the GDPR, do contact Pippa Halpin 020 7421 4695 pippa.halpin@booksellers.org.uk

8th February 2018

General Data Protection Regulation (GDPR) Top Tip

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security. There are some heavy fines for non-compliance and small and medium businesses are being warned not to ignore it.

Top Tip: Create an Excel spreadsheet listing all of the personal data you hold (often called a **Data Inventory**).

This 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)

You may need to talk to other staff to make sure you've listed everything.

Why bother:

- Knowing what personal data you hold is the first step to meeting many other GDPR requirements.
- For example, to update inaccurate data/ delete out of date data/ give customers access to their data if they request it, you will need to know what personal data you have, who else has it and where it is stored.
- The GDPR has an 'accountability principle': you need to be able to *show* how you comply with the GDPR. A Data Inventory is a first step towards that.

The key place to go for more information is the Information Commissioner's Office (ICO) website www.ico.org.uk. The ICO have many helpful GDPR resources for small and medium businesses, including a new advice service helpline. Click here for their GDPR guides, checklists and steps to take now.

If you have any questions about the GDPR, do contact Pippa Halpin 020 7421 4695 pippa.halpin@booksellers.org.uk

13th March 2018

General Data Protection Regulation (GDPR) Top Tip

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security. There are some heavy fines for non-compliance and small and medium businesses are being warned not to ignore it.

Top Tip: Update your Privacy Notice.

Why bother:

- Individuals have a 'right to be informed' under the GDPR about who you are and how you are using their information: this is usually done through a Privacy Notice (previously called a Fair Processing Notice) which can be easily accessed on your website.
- Transparency through a Privacy Notice is a means of building trust and confidence with your customers.

You may already have a Privacy Notice on your website: if not, you should create one. Under the GDPR, there are some additional things you have to tell your staff, customers and suppliers in your Privacy Notice.

Information to be supplied includes:

- The identity and contact details for your business and your data protection officer
- The purpose of the processing and the legal basis for the processing (eg. 'We collect your personal data to help us order and deliver your purchases, as well as to promote our services to you. We use your data either to fulfil a contract with you, or as a result of your consent.')
- Categories of personal data (eg. 'We collect customer names and phone numbers.')
- The right to withdraw consent at any time, where relevant (eg. 'Personal information may be used as a result of your direct consent: in these instances, you have a right to withdraw consent at any time.')

You will need to check the full list on the ICO Privacy Notice code of practice to ensure you've included everything.

Click here for the ICO GDPR guides, checklists and steps to take now. Pippa Halpin will be at the BA Stand 4A41 at London Book Fair (10th – 12th April) to help answer any GDPR queries.

27th April 2018

Data Protection - GDPR FAQs for BA members

The EU's General Data Protection Regulation (GDPR) is coming into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security.

The BA have produced a **GDPR FAQs** document for booksellers which can be found here.

If you have any questions about the GDPR, do contact Pippa Halpin 020 7421 4695
pippa.halpin@booksellers.org.uk

General Data Protection Regulation (GDPR) Top Tip

Top Tip: Review how you manage consent. Refresh existing consents if they don't meet the GDPR standard.

This might involve:

- Getting familiar with the six lawful bases for processing personal data, and recording in your Data Inventory when you are relying on 'consent' as the lawful basis for using a customer's/supplier's/staff member's personal data
- Double checking that 'legitimate interest' is not a more appropriate lawful basis: this is the most flexible lawful basis and can be used for marketing activities instead of 'consent', but it comes with some additional considerations
- Checking that previous consent from customers/suppliers/staff was 'opt-in' (e.g. no pre-ticked tick boxes, no 'unless you tell us otherwise, we'll sign you up for…')
- Checking that you've told people what you are going to do with their data (e.g. 'We'll use your email address to send you our fortnightly newsletter')
- Checking that you've given separate 'granular' consent options (e.g. a tick box for your fortnightly newsletter, a tick box for emails about your book club, a tick box for emails about offers from other local businesses)
- Checking that you've told people they can withdraw their consent at any time and that you've made it easy for them to withdraw their consent (e.g. include an 'unsubscribe' option in your mailings)
- Checking that all of this is in clear, plain language
- Checking that you have a record of how and when you got consent from the individual (e.g. keep files with hard copies of sign-up forms, check that your online systems capture the date and time someone signs up)
- Ensuring that you will gain fresh, GDPR-compliant consent if you aren't currently meeting the above GDPR standards. This might require a mail out to current customers, asking them to confirm they would like to stay on your mailing lists. Mailchimp have some guidance on how to collect GDPR-compliant consent with their sign-ups forms.

You will need to check the full list of requirements on the ICO Consent Checklist to ensure you've covered everything.

Click here for the ICO GDPR guides, checklists and steps to take now. Click here for the BA GDPR guides, FAQs and top tips. If you have any questions about the GDPR, do contact Pippa Halpin 020 7421 4695 pippa.halpin@booksellers.org.uk