Heart Internet Presents

THE RESELLER'S GUIDE TO

DATA PROTECTION

Strong data protection is important for your business. Find out what you need to do with this guide from Heart Internet.

Heart Internet

The Reseller's Guide to Data Protection

Privacy is important to your customers. They need to know that their details are stored safely and that you, as a business, value their privacy and their personal information.

Strong data protection, including what is needed for GDPR, is important for any business – not just for following legal requirements, but also for building trust with your customers and helping your business to grow.

Please keep in mind that **this guide is not meant as legal advice**, and is not an exhaustive list of data protection requirements. To determine exactly what is required of your business to ensure your compliance, please speak to your solicitor.

What is GDPR?

The General Data Protection Regulation (GDPR) is a set of regulations designed to put the highest levels of protection around personal data. It's built to give consumers ultimate control over their own personal data and what happens to it.

There are four customer rights and four company obligations that GDPR brings into play:

Customer Rights

Transparency – The right for individuals to know what is happening with their personal data.

Consent – The right for individuals to choose what personal data is collected about them and to change that choice when they decide to.

Update and Erasure – The right for individuals to update or request deletion of their personal data.

Portability – The right for individuals to request a machine-readable copy of their personal data.

Company Obligations

Due Care – That companies safeguard personal data.

Minimisation – That companies only collect personal data that is necessary for its intended purpose.

Privacy by Design – That companies analyse what risks affect personal data and work to minimise those risk

Notification – That authorities such as the Information Commissioner's Office are notified as soon as possible of any data breaches that affect personal data.

Personal data is any information that relates to an individual that can directly or indirectly identify the individual. Some of the examples provided include:

- Name
- Photo
- Email Address
- Bank Details
- Physical Address
- Cookies on a website
- Computer IP address

In order to be compliant with GDPR, businesses must handle personal data as carefully as possible, as well as providing their users with ways to control, check, and delete any personal information the business holds.

Businesses must also have processes in place to ensure that data is always protected and kept secure. As a business, you will need to regularly conduct privacy impact assessments, strengthen how you seek permission to use the data, document exactly how you will use the data, and improve the way you communicate any potential data breaches.

If you collect, store, or use any personal data of any EU citizens, no matter where you are located, you will be affected by GDPR. And failing to comply with GDPR can lead to massive fines.

You can find out more about GDPR from the Information Commissioner's Office [1].

After the United Kingdom leaves the EU, a new data protection law based on GDPR will be introduced, meaning that, even if you do not have EU citizens as customers, you will still need to follow those policies if you have UK customers.

Your customers' personal information

When you gain a new customer, you need to take some basic information, such as name, physical address, email address, and phone number. When they buy products, you collect more information. And if a customer gets in touch with you, you'll have information on how they contacted you, when, and what about.

All of that counts as personal data, and along with deciding what exactly you want to keep and why, you need to explain to your customers what you're keeping, why you're keeping it, and how you will use it.

Not only will you need to explain, in clear language, exactly what you're collecting and how you will use it, but you will also need to keep that data secure, available, and, when asked by a customer, be ready to delete that data.

All customers now have the right to ask for a copy of all personal data you have on them. Within the Reseller Control Centre, you can export all your customer data from your Customer Database. In HostPay, you can export individual customers on the Your Customers page.

And if a customer no longer has any domains, hosting packages, or add-ons under their account with you, they can also ask for all their personal data to be deleted. This will delete all the personal data that we hold within your Reseller Pro account, and we will be unable to retrieve any information from it after it has been deleted.

In the Reseller Control Centre, you can select the customer’s name under Current Contacts and click Delete. In HostPay, view the customer on the Your Customers page and tick the box under the Delete column. Click the Delete button, and the customer will be removed.

Your customers' consent

Consent is a major thing for GDPR. While previous data protection legislation let you assume that your customers passively agreed to receive information, you now must actively receive consent.

For example, while you might have built up your newsletter list by adding anyone who downloaded an e-book, you now need to provide clear and obvious subscription options wherever you ask for an email address.

You also need to make certain that your existing lists are populated entirely only by people who wanted to receive marketing materials. If you're unsure, you can send out an email to your existing lists, asking them if they want to stay subscribed or not. Then use that list as your master list of clear and informed consent.

Consent obviously doesn't apply to any essential communication, such as invoices, account changes, or emergency calls. But it does apply to any newsletters, promotional emails, mailshots, or sales calls you might make.

Your Reseller Control Centre does have an option to email all your customers, but it doesn't store their consent decisions. It should therefore only be used for essential communication, not for any marketing purposes.

You can also break up the levels of communication consent even further. Perhaps you will have customers who want to receive your regular offers, but don’t want to receive a monthly newsletter. Or customers who like reading the newsletter, but aren’t interested in any new products. Customers who are happy to receive telephone calls as well as emails versus customers who only want to be contacted via email.

By ensuring you have clear and direct consent to communicate to your customers, you will have an engaged audience who are actively looking for your content. And more engagement means more results.

Organising your invoicing and billing

Your customers' invoices are obviously an important part of your business. But with your customers' personal data on the invoices, such as name, email address, and physical address, not to mention your own personal data, they can provide a bit of a tricky situation for anyone focused on data security.

Invoices should first be divided into two categories – paid and unpaid. Unpaid invoices are obviously kept available and around, even if a customer requests the deletion of their personal data. You need this invoice not only for your records, but also to receive payment.

Paid invoices are gradually archived and then deleted, with customers able to also remove their invoices. The schedule for paid invoices is:

Less than 2 years – Invoices are available to the customer and to your company to review as needed

2 to 7 years – Invoices are securely archived, viewable by your company, and can be retrieved as needed for customers

Over 7 years – Invoices are deleted from the system and cannot be retrieved by your company or your customers

With your invoice archive, you will need to make certain that it is well managed and kept secure. If you have electronic records, make certain that there are procedures in place for checking in and out records and that the invoices remain unchanged and untampered. If you have paper records, you will also need to make sure they are in a secure location physically, such as a locking file cabinet or external storage rental.

ICO has a checklist for records management that can help you ensure that your invoices and other important records are kept secure. **[2]**

Using cookies and other tracking scripts

Cookies let you deliver the best service to your customers, helping keep them logged in and matching their preferences. However, cookies can be used for marketing purposes, such as retargeting advertising and analytics, and, as such, must be agreed to by your visitors.

You may have seen many sites with a generic "Our website uses cookies" statement. There now needs to be active acceptance of cookies from your visitors. You can also specify which cookies visitors can accept or decline, giving people a chance to agree to live chat, but not to advertising.

If you use HostPay, the basic version of the site does not include any tracking cookies and you do not need to ask your visitors if they want to manage their settings. However, if you have added any other cookies, such as Google Analytics, you will need to notify your visitors.

Creating a privacy policy

The privacy policy is one of the most important things you need on your site. While many people will not bother to read it, it gives every visitor a chance to see exactly what you hold, how you use it, and how you store it.

Your privacy policy needs to be in clear and understandable language and list everything that you do to keep visitor data secure. You don’t need to get down into the technical jargon, but you need to make it clear to visitors that you have taken all the steps necessary to protect their personal data and will not abuse it.

If you use external systems to process your data, you will also need to create a list of who they are, what they do, and what data they have access to. This does not need to be in your privacy policy, but it does need to be available if customers ask for it.

ICO have produced a checklist for a privacy policy, which may be helpful. **[3]**

More information

There are plenty of resources online about data protection and the GDPR.

The single most important one is the Information Commissioner's Office. Their site for organisations is detailed, easy to read, and will give you the information you need to make sure you are covered **[4]**

There is also a GDPR Checklist you can go through and see whether or not you have completed necessary actions. **[5]**

The Institute of Electrical and Electronics Engineers have also produced a guide to GDPR which gives you more information and a glossary of terms used. [6]

Heather Burns, a digital law specialist, has also written an article for Smashing Magazine about GDPR and how it can affect developers. **[7]**

We have also produced two blog posts, one a general guide to what you need to do **[8]**, and another focusing on frequently asked questions **[9]** you might have about how we are compliant with GDPR.

Resources

[1] Information Commissioner’s Office – Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

[2] Information Commissioner’s Office – Records Management Checklist
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/records-management-checklist/

[3] Information Commissioner’s Office – Your Privacy Notice Checklist
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/your-privacy-notice-checklist/

[4] Information Commissioner’s Office – For Organisations
https://ico.org.uk/for-organisations/

[5] Gertjian De Wilde, Willem Delbare, and Johan De Keulenaer – The GDPR Checklist
https://gdprchecklist.io/

[6] Rosa Maria Garcia Sanz, Institute of Electrical and Electronics Engineers – Your Guide to GDPR
https://spectrum.ieee.org/telecom/internet/your-guide-to-the-gdpr

[7] Heather Burns, Smashing Magazine – How GDPR Will Change The Way You Develop
https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/

[8] Heart Internet – A guide to GDPR and what to do to prepare
https://www.heartinternet.uk/blog/a-guide-to-gdpr-and-what-to-do-to-prepare/

[9] GDPR and Heart Internet: Frequently Asked Questions
https://www.heartinternet.uk/blog/gdpr-and-heart-internet-frequently-asked-questions/