and

The General Data Protection Regulation

(GDPR)

Information for Data Controllers / Bunting Customers

Last updated: 15th February 2018

Introduction

This document details how Bunting complies with the GDPR, and how our customers can ensure they are compliant with GDPR when using Bunting.

Bunting has been preparing for GDPR since early 2017. We have had a full data protection audit, working with data protection lawyers to ensure total compliance. Our processes and our software have been updated to meet GDPR requirements since mid 2017, well before the deadline.

We are more than happy to speak to our customers and advise on best practice for GDPR.

If you feel any of your questions haven't been answered by this document, get in touch: gdpr@bunting.com - we'd be happy to answer them.

Definitions

Here are some definitions that will help in understanding this document.

Data controller Referred to as ‘controller’. This refers to a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. Bunting acts as a controller for internal data such as HR records, sales data and customer data.

Data processor Is referred to as ‘processor’. This means any person/organisation (other than an employee of the data controller) who processes data *on behalf* of the data controller. There may be more than one or several; and these are often software vendors eg. marketing automation or personalisation providers. In our case, Bunting’s software tool is a processor, as we process data on behalf of the controller, our clients.

Individuals Used to describe data subjects and sometimes referred to as ‘natural persons’ within the GDPR framework.

Personal Data Any data that can be used to identify an individual such as name or email address. This definition is broader under GDPR and includes IP address, as this can potentially be identifiable information.

Person Data Any data related to a person, including anonymous data.

The GDPR

What is the GDPR?

The General Data Protection Regulation (GDPR) comes into force on the 25th May 2018, and supersedes the previous Data Protection Act.

It affects any company that stores or processes the personal data of EU citizens. The GDPR only applies to *personal* data, which is any kind of data from which an individual could potentially be identified.

This applies to both data controllers and processors (Controllers, in this case, being our customers, and the processor being Bunting). Businesses need to ensure compliance and, importantly, to document *how* they comply with the new regulation.

The ICO gives a useful summary of the 12 steps that need to be taken:
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The full version of the GDPR can be found here:

REGULATION (EU) 2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,and repealing Directive 95/46/EC
(General Data Protection Regulation)
http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

Data Processing

Why does Bunting store personal data?

Bunting provides a Software as a Service (saas) real-time marketing personalisation system which holds data about ecommerce customers and website visitors.

Bunting acts as a data processor and plugs into websites (the data controller), to improve the website experience by displaying personalised content, such as messaging relevant to a website visitor's region, or product recommendations relevant to the individual's interests. In order to carry this out, Bunting holds a small amount of personal data - but only that which is necessary.

The majority of the data collected by Bunting is not personal. If an individual returns to a website several times or purchases a product, then a small amount of personal data will be stored by Bunting in order to perform its software function.

What personal data does Bunting store?

Bunting uses behavioural data (on the products and pages an individual views) to predict what content the visitor will want to see in the future. If a customer fills out a form on the controller's site, then Bunting will record some of that data, some of which will be personal, as detailed below. Bunting does not hold any sensitive data of any sort.

The Bunting software tool holds the following types of data on our clients' website visitors and customers.

Personal data	**Other data**
Name (if entered onto the site)	Onsite behavioural data - Products and pages browsed; Products purchased.
IP address	
Email address (if entered onto the site)	

Who has access to personal data?

The personal data stored within Bunting can be accessed by a small number of Bunting's employees who only require access to the data in order to perform their work duties ie. to ensure the system is working correctly. Data is anonymised where possible.

All Bunting staff are trained in GDPR and data protection to ensure the integrity and protection of personal data as detailed in section 2.

Bunting users can set user privileges so some staff cannot see personal data. We advise changing these user privileges - if it is not necessary for certain staff to see personal data, then stop them from seeing it. You can do this through technological measures where possible, supplemented by training and changing your business processes.

How Does Bunting Handle Data Security?

We take every measure to ensure that the data held by Bunting is secure to the utmost level. We do that in the following ways:

- Bunting's data (including personal data) is stored on the Amazon AWS Cloud, using MySQL databases. EU data is stored within the EU Economic Area, on our AWS servers in Ireland. World-renowned, reliable physical security is implemented by Amazon and database security is implemented by MySQL.

- Every Bunting account has its own dedicated, isolated database. For our customers, this means added security of having visitor data completely isolated from every other account on our network.

- All data is held on servers audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available.

- All backups are encrypted as standard practice, and Bunting is routinely penetration tested.

Retention Period

In line with GDPR, Bunting routinely deletes aged data when it is no longer useful. Personal data is not kept for longer than is necessary for its purpose.

Bunting Data Protection Impact Assessment (DPIA)

Bunting has carried out a DPIA in consultation with our data protection lawyers which was found to meet GDPR principles.

What is Bunting's Lawful Basis for Data Processing?

There must be a Lawful Basis for processing Personal Data under the GDPR, which needs to be documented. Bunting has outlined its lawful basis for the processing of personal data as set out in Article 6.1.

For more information visit:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

For email marketing, we must rely on:

CONSENT – individuals must give their Consent to the processing of their Personal Data in order to send email communications. This doesn't apply to emails that are necessary (such as order confirmation emails), but does apply to marketing emails.

For personalised on-site content, such as product recommendations, our lawful basis is:

LEGITIMATE INTERESTS – When using this basis, you don't need consent. On-site personalisation is necessary for the purposes of legitimate interests pursued by the controller (our clients) or a third party, in making their websites more relevant to visitors, *unless* these interests are overridden by the individual's interests or fundamental rights.

How to Implement GDPR Processes and Individuals' Rights

We have made changes to both internal processes and to our software tool to ensure we are meeting the full demands of the GDPR.

This section will advise how to include Bunting in your GDPR preparations.

Communicate privacy information

You must update and display your privacy information detailing how and why you collect personal data in **clear and unambiguous language.** More information can be found under the 'Rights for Individuals' below.

Consent

You must obtain consent from your customers in order to send email marketing communications. This **must** be an affirmative opt-in (not a pre-ticked box).

Before you can use Bunting's email tools, Bunting must know that consent has been given for each recipient. By default, Bunting sets all new visitor's email subscription statuses as being opted out ('optout'). However, you can update this to 'subscribed' by telling Bunting via a copy/paste Javascript tag ($_Bunting.d.ess), which you can find on the Installation > Tracking Code page. (NB: this feature will be live March 2018)

Obtaining consent for on-site personalisation using Bunting is not necessary if using Legitimate Interests as your legal basis. However, we recommend you seek your own legal advice for your marketing activities.

New Rights for Individuals

Any data subject in the Bunting system who wishes to exercise their rights under the GDPR can do so easily.

If you wish to contact us with regards to a data subject access request, you can contact us at gdpr@bunting.com. This information will also be displayed on our website.

Please see below for how Bunting complies with the new individual rights under GDPR and to see how you can implement the rights of your data subjects. Data subject requests should be dealt with within 24 hours and you should not charge for this.

i. The right to be informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

The information you supply about the processing of personal data must be:

- *concise, transparent, intelligible and easily accessible;*
- *written in clear and plain language, particularly if addressed to a child; and*
- *free of charge*

ICO, 2017
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/

All Bunting customers using Bunting must display privacy statements covering all the required information. You should consider the following for your privacy pages:

- Personal data may be used to personalise marketing and on-site content such as product recommendations.
- Personal data may be used to send triggered emails.

ii. The right of access

Under the GDPR, individuals will have the right to obtain:
confirmation that their data is being processed; access to their personal data; and other supplementary information
ICO, 2017
https://ico.org.uk/for-organisations/data-protectionreform/overview-of-the-gdpr/individuals-rights/the-right-ofaccess/

Bunting clients can deal with visitors'/customers' right of access requests as follows:

On logging in to your Bunting account, you can search by email address for the individual concerned and be able to send the data to the subject. You can do this by copying-and-pasting their data from the screen into your response.

iii. The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
ICO, 2017
https://ico.org.uk/for-organisations/data-protectionreform/overview-of-the-gdpr/individuals-rights/the-right-torectification/

Bunting has built the following into the software for compliance:
We request that Bunting users correct the data in their own e-commerce system. Then, we request that they search for the individual within the Bunting system and **delete** the record. Bunting will automatically scrape the correct data for them from their website in the normal way.

Any individual who wishes for Bunting to rectify their personal data can do so by contacting gdpr@bunting.com, as outlined on the Bunting website. Their data will be rectified free of charge.

iv. The right to erasure

The right to erasure is also known as 'the right to be forgotten'.
ICO, 2017
https://ico.org.uk/for-organisations/data-protectionreform/overview-of-the-gdpr/individuals-rights/the-right-toerasure/

Bunting has a 'delete' function which means individuals' data can be deleted, and the individual can be considered 'forgotten'. If an individual makes a request to have their data deleted then the Bunting user can simply search for the individual within Bunting's 'Visitors' section, and select the option to 'Delete Personal Data', erasing all data.

Remember this should be done within 24 hours of the request and free of charge.

v. The right to restrict processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data.
The restriction of processing under the GDPR is similar. When processing is restricted, you are permitted to store the personal data, but not further process it.
You can retain just enough information about the individual to ensure that the restriction is respected in future.
ICO 2017
https://ico.org.uk/for-organisations/data-protectionreform/overview-of-the-gdpr/individuals-rights/the-right-torestrict-processing/

Bunting has built in new capabilities to ensure GDPR compliance. Data controllers (Bunting users) can deal with the right to restrict processing requests as follows: within the 'Visitors' section, search for the profile of the individual, and select the option labelled 'Restrict Processing'.

vi. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
ICO, 2017.
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/

Bunting customers can deal with data portability requests as follows: Use Bunting to search by email address for the individual and copy-and-paste their data from the screen into your response. It is in HTML or JSON which are structured, commonly used and machine-readable forms which will allow portability.

vii. The right to object

Individuals have the right to object to:

- *direct marketing (including profiling);*

If you process personal data for direct marketing purposes:
You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse. You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

ICO, 2017
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-object/

You must cease the profiling of an individual **as soon as** an objection is raised. To do this, search for the individual's email address in your Bunting account and press the button labelled "Do Not Process (GDPR)".

Individuals have a right to object and report to their data supervising authority. In the UK, this is the ICO, and details can be found at www.ico.org.uk

viii. Rights in relation to automated decision making and profiling

Rights in relation to automated decision making and profiling. The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
ICO 2017
https://ico.org.uk/for-organisations/data-protectionreform/overview-of-the-gdpr/individuals-rights/rights-related-toautomated-decision-making-and-profiling/

Bunting is unaffected by this right, because the right applies when a decision has a legal or similarly significant effect on someone, which is not the case with Bunting's profiling.

Decide how to verify identification

It is important you verify the identity of individuals when data subject requests are made.

We recommend responding to requests to the email address attributed to the data subject's account, and request photo ID if necessary.

Data Breach Response

Bunting has stringent systems in place to detect and report personal data breaches. In the event of a breach, we will contact all of our clients immediately and advise as to how to inform and protect the affected individuals. If you suspect a data breach in your systems, contact us.

Our Clients' Personal Data

We store small amounts of personal data on our clients for transactional and communication purposes. If you would like to contact us about your own personal data, please contact: gdpr@bunting.com

This document will be updated in line with changes to the GDPR.

If there's anything we haven't answered in this document, contact us at gdpr@bunting.com

Bunting Software Ltd

101 Princess Street,
Manchester
M1 6DD

bunting.com