Fresh Relevance Support for the General Data Protection Regulation (GDPR).

Introduction

If you want to contact us about your personal data, see the first page here.

Fresh Relevance has supported the GDPR since 25 May 2017, 1 year before it becomes law.

This document introduces the GDPR, describes how Fresh Relevance provides a high level of security for personal data, and documents what clients should do to make sure that their implementation of the new individual rights also covers personal data stored in the Fresh Relevance system.

It is written by Peter Austin, Data Protection Officer, Chief Innovation Officer and Co-Founder.

The content of this document will change to reflect changing official advice about the GDPR. This version is dated 16/01/2017. You can find the latest version here: https://www.freshrelevance.com/contact/legal

What is the GDPR?
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

Descriptions of the General Data Protection Regulation (GDPR)
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Overview of the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/data-protection-reform/

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

https://ico.org.uk/for-organisations/data-protection-reform/useful-links/

This is important: The GDPR [only] applies to personal data of an identified or identifiable natural person. *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."*
http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

Supporting the GDPR involves the steps summarized here.
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Data Controller and Data Processor

Each client is the Data Controller for their data and Fresh Relevance is one of their Data Processors.
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/

"data controller" means 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. There is usually only one.

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. There may be several.
https://ico.org.uk/media/1546/data-controllers-and-data-processors-dp-guidance.pdf

Security of Personal Data

Fresh Relevance provides a Software as a Service (saas) real-time marketing system which holds data about individual shoppers. We call this **person data**. A small amount of this person data may also be **personal data** and relevant to the GDPR, but most of it records anonymous visits and is not personal.

Person Data (including personal data) is stored on the Amazon Cloud, using MongoDB databases. Physical security is implemented by Amazon and database security is implemented by MongoDB. These are both big players and I am confident that they will fully comply with the security requirements of GDPR.

Further security is added by Fresh Relevance and we use several strategies:

1. **Person data (including personal data)** is held in a separate database for each of our clients, so one client cannot access the data belonging to another client.

2. **Fresh Relevance stores very little personal data overall. Most person data (data about people) that we store is not personal data**:

    - Fresh Relevance is a real-time marketing system, not an e-commerce system, so we do not store sensitive personal data, such as passwords, credit card numbers, social security numbers etc.. We store shopping behavior and *optionally* a few items of personal data such as first and last name and email address.

    - The GDPR only considers data to be personal if the person is reasonably likely to be identified and that's not the case with most visitors/shoppers. Real-time marketing such as website personalization works fine with unidentified visitors – we need information about their behavior, not who they are.

      If an anonymous person keeps returning to a client's website, then eventually we will identify them, so their data may therefore become personal. A client can speed up this identification by loading their customer list into Fresh Relevance, or by including ids on click-through links from their marketing emails. But the basic point is that most visitors to a typical website are unidentified and unlikely to ever be identified, so their data cannot be personal.

    - Most of our person data is technical. For example, the exact prices and descriptions of all products seen by a person. This detailed data tells you nothing personal, so it is not personal data.

3. **Fresh Relevance automatically minimises person data.** Fresh Relevance routinely deletes aged data when it is no longer useful. For example, the full data of incoming events is deleted after a short while.

4. **Additional Data Security**. Backups are encrypted. We commission penetration testing and implement its suggestions. We do lots of activity monitoring, including live screens of server activity on our office wall.

In addition, Fresh Relevance Ltd also stores personal data for our own standard business administration. For example, if you ask us a question by email and include your name, that information including your name will be stored. For simplicity, the document that you are reading is only about data held by the Fresh Relevance real-time marketing system. Contact support if you want more information.

GDPR Processes and Implementing Individual Rights

This section will help you include Fresh Relevance in your processes for dealing with the GDPR. Also see Fresh Relevance GDPR Information for Data Controllers.

I have followed ICO's checklist and headlines and quotes are from there: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Awareness of the GDPR within your organization

This is the responsibility of our clients.

- **Information you hold**

  You should document what personal data you hold, where it came from and who you share it with.

  Data held by Fresh Relevance is scraped from our client's website pages, optionally loaded by them using the integration capabilities, or passed in the query collection of click-through URLs. All Fresh Relevance data for EU and UK clients is stored and processed in the EU, using Amazon Web Services (AWS) as the data processor. Data is shared with our client and their third-party systems, such as their ESP and e-commerce system.

- **Communicating privacy information, Legal basis for processing personal data** and getting **Consent**.

  Privacy notices are the responsibility of our clients. You should tell clients what you are going to do with their data, briefly and simply.

  We believe that triggered emails *sent as part of your normal purchase processing* do not need separate GDPR permission; they are covered by your legitimate interest. You just need to warn shoppers that they will be contacted and make it easy for them to unsubscribe. For example, cart and browse abandonment emails, post-purchase order details, delivery reminders, servicing and consumables reminders.

  Some additional marketing, including bulk email such as newsletters, is not part of normal purchase processing, making it more intrusive. This does need separate permission. If you are asking for this permission on your purchase form, you should use a separate checkbox or pair of radio buttons for each additional type of marketing.

  Personalization and product recommendations (whether Web or Email) do not need separate permission - they are allowed as your legitimate interest.

  Strictly speaking you can claim two legitimate interests: Marketing is necessary for the purposes of legitimate interests pursued by the controller or a third party, because companies exist to sell stuff – see 6(1)(f). And marketing is in the public interest, because it grows the economy and tax base, which improves all our lifestyles – see reference 6(1)(e). But note that I am not a lawyer and you should get your own advice on the GDPR https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/

- **Children**. If any of our clients specifically targets child customers, it is their responsibility to verify ages and to gather parental or guardian consent.

- **Data breaches**. Fresh Relevance has procedures in place to detect, report and investigate personal data breaches – either in the Fresh Relevance system, or the client website that it integrates with. (It is not our job to do so, but our monitoring has in the past detected attacks by third parties against a few of our clients.)

  If we detect a data breach or other attack, we will inform our client, so that - as Data Controller - they can take control of informing affected individuals and the authorities. As Data Processor, we also have the responsibility to make sure that these parties are informed, but we prefer it to be done by our client. We will only contact third parties directly in exceptional circumstances, for example if our client does not do so reasonably promptly.

- Data Protection Officer

  Peter Austin, Chief Innovation Officer and Co-Founder, Fresh Relevance Ltd
  Please contact by email: gdpr@freshrelevance.com
  https://www.freshrelevance.com/contact
  https://www.freshrelevance.com/meet-the-team

- Fresh Relevance Ltd is regulated by the UK data protection supervisory authority. https://ico.org.uk/

  We expect that BREXIT will proceed slowly and not affect this for 5+ years.

- **Individuals' rights** including **Subject access requests**.

  Note 1: Our approach is mostly manual, because in our experience previous data protection rights were used extremely infrequently (less than once per week per 10 million people) so automation is not worthwhile. But if people use their new rights very often, we will consider fully automating them.

  Note 2: if someone contacts you to enforce their rights under the GDPR, it is your responsibility to make sure they are who they claim to be and not a criminal trying to hijack an account. I don't think the ICO has provided guidance on this yet, but the principle is that you ask them to do something that only a real customer can do. Suppose you know the email address: if a customer contacts you by phone, you could send a unique code to the email address in your records and ask them to call back once they have received it and read it back to you.

  [1] Note 3: In the following, "Use Fresh Relevance to search by email address for the person" means: Logon, click Reports | Reports Home | Shoppers, enter their full email address and click Search.

  The GDPR provides the following rights for individuals...

- **The right to be informed**

  The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasizes the need for transparency over how you use personal data.
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/

  You should consider adding the following to your privacy page:
  - Personal data may be used to send triggered emails, such as cart abandonment and purchase confirmation emails.
  - Personal data may be used to personalize marketing, for example to suggest products that are related to your previous purchases.

- **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
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-of-access/

  Use Fresh Relevance to search by email address for the person[1], click the "download" button to retrieve their data, and attach it to your response. The data format is JSON which is a structured, commonly used and machine-readable format. There is also an API call to retrieve person data. Contact us for more information.

- **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.
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-rectification/

  Correct the data in your e-commerce system. Then use Fresh Relevance to search by email address for the person[1] and delete them. Fresh Relevance will automatically collect correct data for them from your website as they use it, in the normal way.

- **The right to erasure**

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

  Delete the person from your e-commerce system. Then use Fresh Relevance to search by email address for the person[1] and delete them.

- **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.
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-restrict-processing/

  Use Fresh Relevance to search by email address for the person[1] and press the button labelled "Do Not Process (GDPR)". There is also an API call to set do not process.

- **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. You must provide the personal data in a structured, commonly used and machine readable form…

  This right does not apply to most person data, for example not the log of which marketing and products each individual has seen. *It only applies:*
  • to personal data an individual has provided to a controller;
  • where the processing is based on the individual's consent or for the performance of a contract; and
  • when processing is carried out by automated means
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/
  https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

  Use Fresh Relevance to search by email address for the person[1], click the "download" button to retrieve their data, and attach it to your response. The data format is JSON which is a structured, commonly used and machine-readable format. There is also an API call to retrieve person data. Contact us for more information.

- **The right to object**

  Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-object/

  Use Fresh Relevance to search by email address for the person[1] and press the button labelled "Do Not Process (GDPR)". There is also an API call to set do not process.

- **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.
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/rights-related-to-automated-decision-making-and-profiling/

  Fresh Relevance is unaffected by this right, because *the right does not apply when a decision does not have a legal or similarly significant effect on someone*. The processing that we do is not important enough to reach that threshold.