freshrelevance

Fresh Relevance support for the GDPR

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 became 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 8/7/2021. 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/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Supporting the GDPR involves following the process that starts here.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

Multiple GDPRs following Brexit

When the UK left the EU, it cloned the GDPR into UK law, so now there are…

- the UK GDPR, which applies in the UK
- the original GDPR, sometimes called the EU GDPR, which applies in the EU

These two GDPRs are almost identical. They will slowly drift apart due to court decisions and other legislation, but for now it's simplest to treat them as being the same, so this document will do that (get advice from a lawyer for the precise

details). References:

- https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/
- https://www.osborneclarke.com/insights/uk-eu-data-protection-post-brexit-brief-guide/

Some companies need to specifically comply with both GDPRs, for example because they deliberately target customers in both the EU and the UK. One issue for them is if they only have a physical presence in one place, such as an office with staff, because then they may need to appoint a GDPR representative in the other. As an example, here is what we tell people:
https://www.freshrelevance.com/eu-representative

Data Controller and Data Processor

Each client (website owner) 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 personalization and personification system which holds data including marketing and website visits. We call this **person data**.

Person Data (including personal data) is stored on our AWS servers, using MongoDB databases. The database servers are not internet-accessible, data is encrypted in flight and at rest, there are copies on two availability zones (in separate buildings), and backups are taken frequently. Physical security and backups are implemented by AWS and database security is implemented by MongoDB, which are both big players and our storage complies 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.

      For reference, here's the relevant quote that 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

    - 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 useful about the person, so it is arguably not personal data, in the same way that a UK weather report tells you about the weather experienced by a person in the UK without being 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**. For example we have implemented the UK government standard, Cyber Essentials.

In addition to the data held by our personalisation system, 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 followed ICO's checklist and the headlines and advice are from there, while the responses relate to Fresh Relevance. ICO has since reworded their content so there's no longer a single checklist, but the same information is here: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

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* (also known as transactional emails) 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 websites 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

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

Data Subject Rights and Subject Access Rights

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

  The GDPR provides various rights for individuals, that they can contact you to obtain, for example the right to request a copy of their data that you hold. These are described in our related document, "GDPR Information for Data Controllers", which is on our legal page, so for details read that.

  NB: if someone contacts you to request 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 e.g. hijack an account. I don't think the ICO has provided good guidance on this, but the principle is that you ask them for something that only the genuine person can do. Suppose you know their 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.

Other Links

The following reference pages help you to find which privacy laws apply to you and your customers, or provide country-specific advice. Note that there are differences even between between EU countries that theoretically share the same GDPR.

- Data Protection Laws around the world, a clickable map from DLA Piper.
- Data protection registrars around the world, a clickable map from CNIL (the regulators provide advice).
- Privacy Laws by Country, brief descriptions from privacypolicies.com.
- Data Protection Laws, Acts or Regulations, a list with links to the legal texts, from michalsons.
- Direct Marketing in Germany, where double-opt in is required for marketing emails, from TaylorWessing.