GDPR Compliance and Commerce **Search & Browse**

By EmpathyBroker Personal Data Committee

December 2017

- Rev: 14th January 2018- Added Detail of EB Products (Contextualize & Empathize).

- Rev: 31st January 2018 - Extended introduction and context.

- Rev: 2nd February 2018 - Added images and detail abstracting from EB Products to general Search & Browse functionality (to map value to both EB SaaS and Services/OEMs clients and partners).

Table of Contents

Executive Summary

Within the context of **Commerce Search & Browse**, User Interfaces, APIs and Reports do not necessarily depend on **Personal Data** to function.

However, some recent advancements such as one-to-one **Personalisation** may be affected by GDPR.

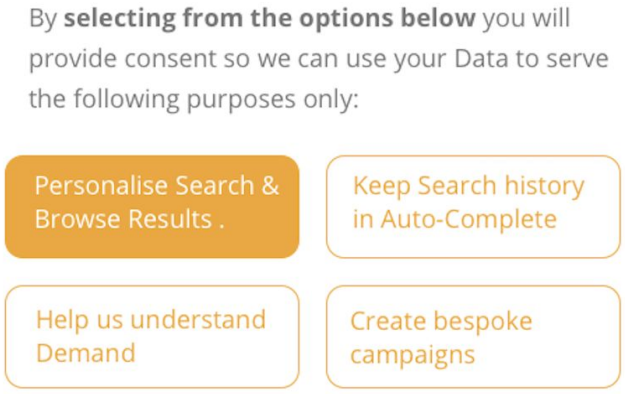
Direct to point: What changes?

Before unfolding the detail of this paper, **what's the change?**

Search & Browse in Commerce shall be understood as involving three separated by unified areas:

1. User Interfacing
2. Search APIs or features
3. Reporting or Insights

The GDPR Directive, once mapped to specific EU States legislation, will most probably imply the introduction of **new Consent forms.**



Sample Consent to activate advanced Search Functionality when Personal Data may be participate.

The User or Consumer will have to explicitly select and **ACCEPT** to share her or his Personal Data to whatever purposes and trusted partners (Personal Data Processors) the online store (Personal Data Controllers) states with openness, transparency and clarity. No hidden purposes.

When a User declines or does not explicitly accept (consent) to share Personal Data, this does not imply a removal of standard functioning of any of the components that make Commerce Search & Browse, that is, the User Interfacing, the Search APIS and features and neither the Insights or Reports that are produced.

However, and beyond the basic functioning of Search there are some **recent developments in Machine Learning, Data Automation or Artificial Intelligence** (that automate processes such as personalisation based on heavy User Profiling, Geo-location and the like) **that may be affected** by the absence of User Consent.

Some of these recent advancements in Search & Browse that may be affected (which are further detailed in How does GDPR Affect EmpathyBroker User or Context features) are:

- **Personalisation** or Contextualisation in Search (i.e. Contextualize) and whether is General Sorting or One-to-One individualised - which requires Profiling.
- **Personalisation in Auto-Completes** (i.e. Empathize) which runs on Local Storage (freed from GDPR requirements)

More in: How does GDPR Affect Personalisation in Search

About this Paper

This document has been compiled by the **Personal Data Committee** at EmpathyBroker with informational purposes.

The following sections discuss Search & Browse within the context of GDPR, these discussions have been collected as of the date of publication of this paper and are subject to change without notice.

EmpathyBroker makes a set of resources and recommendations aimed at helping its customers to act responsibly. These recommendations are provided without warranties, representations, contractual commitments, conditions or assurances from EmpathyBroker, partners or OEMs, and they are also **subject to each customer's independent assessments.**

This document, therefore, does not modify any agreement between EmpathyBroker and its customers or partners.

About the Personal Data Committee at EmpathyBroker

The Personal Data Committee holds representatives from **every EmpathyBroker product and technology area**. This committee is chaired by EmpathyBroker's Security Officer, holding weekly meetings (prior to 25th May 2018) and by-weekly sessions (after 25th May 2018) in which every EmpathyBroker member, **partners and clients are invited to track Compliance and Opportunities derived from the GDPR and Data Privacy regulations**.

The Personal Data Committee also holds biannual Company auditing (checks) to detect compliance levels, adaptations and changes which are carried out by third party legal auditing teams.

To know more about the Personal Data Committee, joint its sessions or participate (as a client or partner) by getting in touch at:

gdpr@empathybroker.com

Considerations

- The General Data Protection Regulation (the "GDPR") comes to effect on the **25th of May 2018.**
- **EmpathyBroker has been involved in Privacy and Transparency by Design since its conception**, uniquely embracing these Design principles to ensure that EmpathySearch and EmpathyInsights products only use Personal Data for the purposes described at the consent points.
- **EmpathyBroker, as a company, team and product, has completely adopted this approach and carefully follows established parameters for all aspects that are, or could be, sensitive to the notion of Personal Data**. It's from this position that EmpathyBroker presents its clients and partners with the following **recommendations and resources intended to help them prepare for the new regulation and beyond**.

The General Data Protection Regulation

- The new GDPR comes into effect on **25th May 2018**, implementing as per Regulation 2016/679 Of The European Parliament And Of The Council of 27th April 2016.
- The new GDPR is directed at protecting "*natural persons with regard to the processing of personal data and on the free movement of such data*", and **replaces** existing Directive 95/46/EC (General Data Protection Regulation).
- The Directive is intended to **harmonise the various Data protection laws across the EU** through the application of a single data protection law that is binding throughout each member state.
- If an organisation has an establishment in the EU or offers goods or services to citizens in an EU state, then **the processing of Personal Data of the EU residents is subject to this Directive**.

Recommended GDPR articles of particular relevance to eCommerce

Full list available at [Regulation 2016/679 Of The European Parliament And Of The Council of 27th April 2016](#).

Article 5: Principles relating to processing of personal data.

Article 6: Lawfulness of processing.

Article 7: Conditions for consent.

Article 12: Transparent information, communication, modalities for exercise of rights of the data subject.

Article 13: Information to be provided where personal data is collected from the data subject.

Article 14: Information to be provided where personal data hasn't been obtained from the data subject.

Article 21: Right to object.

Article 24: Responsibility of the controller.

Article 25: Data protection by design and by default.

Article 26: Joint controllers.

Article 28: Processor.

Article 29: Processing under the authority of the controller or processor.

Article 30: Record of processing activities.

Article 32: Security processing.

Article 35: Data protection impact assessment.

Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or **statistical purposes.**

GDPR FAQs

- **Does GDPR affect Global companies?**

  GDPR impacts any global company (not just EU companies) who offer goods or services to EU citizens.

- **What's new from the previous Directive?**

  A broader definition of what Personal Data is as it involves any Data that relates to an identifier or identifiable person, direct or indirect.

- **Are IP Addresses and or Location Data considered Personal Data?**

  Yes, location data may all be considered Personal Data and by extension all profiling associated to it.

- **Do any EmpathyBroker products use Personal Data?**

  By default EmpathyBroker platform operation logs store IP Addresses which are considered Personal Data. However, IP Addresses are not necessary for the normal functioning of Search & Browse. Additionally, EmpathyBroker Contextualisation (as personalisation) components do use First party Cookies which are considered to be Identifiers (Personal Data). Disabling Cookies results in disabling One to One Personalisation in Search.

- **What if a natural person (User) does not Consent explicitly to share their Personal Data?**

  As detailed below, in this case EmpathyBroker products will not store IP Addresses nor employ any other form of User Profiling (Cookies) and therefore One to One personalisation would not be enabled.

- **What happens if a company doesn't comply?**

  GDPR penalises non-compliant businesses with fines that are calculated as 4% of annual revenue and there will also be critical brand perception danger that is difficult to quantify.

- **What is the real change in the way I interact with Customers?**

  GDPR is all about clarity and transparently, it's about informing Users about what Data is stored about them and how it's being used together with a means to access this Data (with the option to delete or port it).
  This means ensuring new functionality and derived processes to deliver Consent Forms and on My Activity controls to the natural person.

- **Is offering Users explicit Consent similar to the current Accept Cookies function?**

  It's similar but much more complex as Users must give explicitly informed consent to all uses of their Data as well as have control on how to access this Data. On the Appendix Resources at the end of this document some references and examples are provided.

EmpathyBroker actions for GDPR

EmpathyBroker, as an established UK and Spanish company, has been working with customers and partners on the following areas:

- **Audited EmpathyBroker platform and company** to evaluate and diagnose the required actions to be compliant using an independent third party.
- **Comply** by implementing the required actions as part of the audit.
- **Staff** involvement with a new Security Officer and a Personal Data Committee to therefore separate the Company's Security Officer from the Product's Security Officer.
- **Innovate** beyond compliance in areas such as Privacy by Design for Architectures and Transparency by Design for Experiences and UIs.
- **Share and Communicate** with customers and partners in which ways Data transparency may affect shared interests and the innovation opportunities.

How does GDPR Affect personalisation in Search & Browse?

Today, **online stores use many complex data automation** processes to be more **relevant to every user.**

These tools used in eCommerce to "*Personalise Experiences*" **feed from Cookies** (which constitute "*online identifiers*") and heavily profiled location data such as IPs which **the GDPR explicitly includes** in its Definitions (see Art.4 (1)) as Personal Data.

These tools depend on automated decision making and profiling and these automated decisions can't damage the user, not legally, nor similarly. (See Articles 4(4), 9, 22 and Recitals 71, 72).

GDPR defines profiling as the automated processing that is intended to evaluate personal aspects of the user.

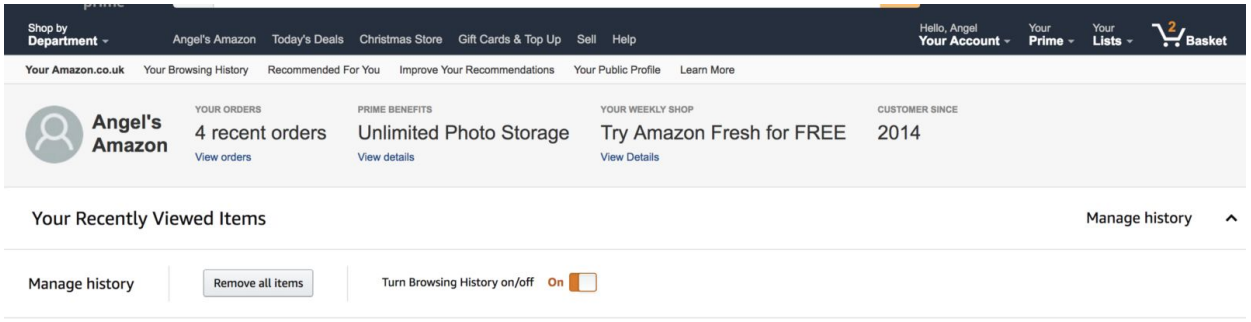
From the pre-defined aspects, these are those that affect eCommerce:

- **Economic Situation:** by tracking User purchases, price percentiles and related calculations.
- **Personal Preferences:** whether captured explicitly or implicitly through tagging.
- **Behaviour:** same as above as affinities for products, brands or categories.
- **Location / Movements:** IPs could be affected (which were already considered, when enriched with the above Personal Data).

Online Stores (as Personal Data Controllers) and Vendors (as Processors), must ensure, when profiling that:

- Processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Some online stores are starting to provide information about the involved logic, look for example at **Amazon Manage History** and how is starting to introduce elements of fairness and transparency.



When a Search & Browse function uses these identifies that may be linked (whether is *pseudonymised* Data) to a natural person, these identifiers shall be recognised as **Personal Data.**

This consideration shall be made regardless of whether the feature uses first party Cookies (under Store Domain) since these are equally used to build End user profiles (or prefered behaviours).

One to One Personalisation in Search	**GDPR (and Data Privacy) key considerations:** 1. Personalisation in Search WOULD NOT activate if the user declines consent (and therefore first party Cookies are NOT available). 2. Personalisation de-activation does not affect the functioning of Search, but the functioning of Personalisation (one-to-one) in Search. 3. Personalisation does necessarily not use Third Party Cookies. 4. Personalisation does not necessarily share Cookies with any other module, component or third party.

One to One Personalisation in Auto-Completes	**GDPR (and Data Privacy) key considerations:** 1. Personalisation in Auto-Completes shall not expose User unique Query Recommendations if Cookies are not enabled. 2. Not populating Auto-Completes with unique Query Recommendations does not affect the rest of functionality Search such as global terms, categories facets or brands.

	3. Auto-Completes don't necessarily need third party cookies. 4. Auto-Completes don't necessarily share Cookies with any other module, component or third parties.

Additionally, **Search UIs (available also as part of EmpathySearch) allow Query History to be exposed from Local Storage,** which does not interact in anyway with the Search Platform (exposing Local Storage to the client only). These Interfaces also offer CLEAR HISTORY options as a means of Clarity, Control and **Transparency by Design.**

Clear History (from Local Storage Sample)

EmpathyBroker recommended GDPR trusted Resources

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
- Guide to the General Data Protection Regulation (GDPR) by the Information Commissioner's Office (UK)

EmpathyBroker produced GDPR articles and commentary

- 2018's turning point: GDPR
- GDPR in eCommerce: The Epiphany of Personal Data
- GDPR in eCommerce: From Compliance to Opportunity

Ways in which EmpathyBroker is evolving this Paper

EmpathyBroker, as an established UK and Spanish company, has been working with customers and partners on the following areas:

- Extending and providing details on each aspect of EmpathyBroker preparations for GDPR.
- Representing workflows of *with* and *without consent* Use Cases for Search.
- Presenting cases for Transparency through Design UI patterns.
- Drafting Data Processing Addendums for Personal Data dependant features such as Personalisation in Search.

www.empathybroker.com


https://twitter.com/EmpathyBro


https://www.facebook.com/empathybroker


https://www.instagram.com/empathybroker/


https://www.linkedin.com/company/colbenson


https://www.youtube.com/user/ColbensonTV


gdpr@empathybroker.com