PRIVITAR

The Right to be Forgotten in the GDPR

www.privitar.com

This paper supports privacy professionals as they respond to Right to be Forgotten (RtbF) requests made to their organization.

The General Data Protection Regulation (GDPR) introduced significant changes. This paper provides an overview of those changes and recommendations on how organizations should respond. It answers five questions:

- What is the RtbF?
- How has the RtbF evolved?
- What additional changes have been introduced under GDPR?
- What guidance is available?
- How should organizations manage RtbF requests?

Introduction

The Right to be Forgotten (RtbF) is not new. It emerged during the 1970s and was codified in a number of legal instruments in the US, Europe and at an intergovernmental level at the Organization for Economic Co-operation and Development (OECD). In Europe, the 1995 Data Protection Directive (95/46/EC) contained elements of the RtbF. The GDPR brought those together as a “right to erasure” and introduced a number of other changes.

This paper:

- Describes the RtbF
- Outlines the changes under the GDPR
- Summarizes the guidance available for organizations and the case law from the Court of Justice of the EU
- Suggests an approach that organizations may want to adopt in responding to RtbF requests.

Organizations should be aware that a similar right exists under the California Consumer Privacy Act (CCPA). The Attorney General, responsible for enforcing CCPA, has stated that de-identifying personal data allows organizations to comply with the right to erasure in the CCPA. As such, the content of this document will be relevant to organizations seeking to comply with CCPA.[1]

[1] Attorney General, CCPA Regulations. Note that the term de-identify carries a specific legal meaning under the CCPA.

How has the RtbF Evolved?

The RtbF is a legal right for an individual to request that a data controller erase their personal information. The right is not absolute; it involves a balancing test and only applies in some circumstances. The balancing test weighs the individual's rights against the controller's interests in processing the data.

It is also called the right to erasure and is one of the OECD privacy principles. The principles are a part of the OECD guidelines on protecting personal data, adopted in 1980.[2] The OECD formulation allowed an individual to *"to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."* Data protection regimes around the world reflect or build on these principles (e.g., the Fair Information Practice Principles in the US or the GDPR and its predecessor the Data Protection Directive in Europe).[3]

The EU's Data Protection Directive (Directive 95/46/EC) enshrined similar rights in its Articles 6, 12 and 14.[4] Article 12 gave the individual the right to *"the rectification, erasure or blocking of data"* where the processing did not comply with the Directive. Crucially, the burden of demonstrating that the processing was non-compliant fell on the individual.

In 2014, the Court of Justice of the EU discussed the RtbF in a case brought against Google.[5] Although the Data Protection Directive does not explicitly provide for a RtbF, the Court ruled that it was a necessary result of the relevant articles of that Directive. The Court's 2014 ruling prompted search engines, including Google, to implement procedures allowing individuals to submit RtbF requests. National regulators, including the ICO, have also published the criteria to use in determining whether a particular search result should be delisted.

It is important to note that the RtbF is not absolute. The Court highlighted the need to balance the data subject's rights, the data controller's economic interests and the interests of the general public in having access to the information cataloged by the search engine.

The Court returned to the RtbF question in a 2019 decision, also involving Google.[6] The case arose from a disagreement between Google and the *Commission Nationale de l'Informatique et des Libertés* (CNIL), France's data protection regulator. CNIL argued that Google had to de-list results globally in order to comply with RtbF. The Court disagreed, holding that there was no legal obligation for global de-listing. However, the Court noted that search engines may nevertheless wish to take measures to "effectively prevent or at the very least, seriously discourage" internet users in a Member State from accessing information that had been de-listed following a RtbF request but was still available on a global search engine site.

[2] OECD, Privacy Principles
[3] Department for Homeland Security guidance on the Fair Information Practice Principles
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[5] Case C-131/12, Google v Agencia Española de Protección de Datos (AEPD)
[6] Case C-507/17, Google v Commission Nationale de l'Informatique et des Libertés (CNIL)

Comparing the Directive and the GDPR

Directive 95/46/EC	GDPR
The data subject had the right to: *"...to object at any time on compelling legitimate grounds relating to his particular situation..."* – Article 14 In order for the data to be erased, the data subject had to show that the data being processed was not: *"...accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"* – Article 6	The GDPR specifies that the data controller *"...shall have the obligation to erase personal data without undue delay where one of the following grounds applies"* It then lists six grounds, including *"(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)"* Article 21(1) reverses the burden of proof, such that: *"The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims."*

Approaching a RtbF Request Depends on How a Company Processes Data

Under the GDPR there are 6 recognized legal bases for processing personal data. How a company responds to a RtbF request will depend on their legal basis for processing, as shown by the table below:

Basis for Processing	Definition	Can a RtbF Request be Rejected?	Under What Circumstances?
Consent	The individual has given clear consent to processing for a specific purpose	No	When customer requests RtbF
Contract	Processing is necessary to perform a contract	Yes	If contract is still in effect
Vital interest	Processing is necessary to protect life	Yes	If data is still relevant
Compliance with legal obligation (inc. legal claims)	Processing is necessary for the controller to comply with a legal obligation	Yes	If data is still relevant
Public interest	Processing is necessary for a task in the public interest	Yes	If public interest outweighs an individual's privacy rights
Legitimate interest	Processing is necessary for the purposes of a legitimate interest, either of the controller or a third party	Yes	If a company's legitimate interest outweighs an individual's privacy rights

When is a Balancing Test Required for RtbF Requests, and What Guidance is Available?

The balancing test is the name for the process by which a controller weighs the interest (public or legitimate) in the processing against the data subject's right to privacy. Companies can reject RtbF requests when the public interest or their legitimate interest outweighs the individual's privacy.

The existing guidance for data controllers falls into four categories:

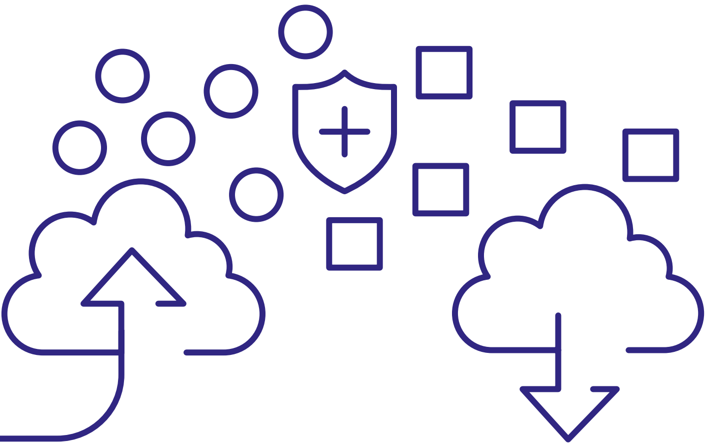
Guidance Type	Definition	Balancing Test Required?	Example of Conditions for Balancing Test
General Guidance on the RtbF	An overview, without specific details on balancing tests.	No	N/A
Search Engines	Weighs individual rights against the broader public interest in access to information	Yes	If an individual is a public figure and whether the information relates to their professional (and not their personal) life.
A Controller's Legitimate Interest	When a Controller has a legal "Legitimate Interest" claim on information	Yes	The ICO guidance: (1) is the interest or purpose of the processing legitimate, (2) is the processing necessary to achieve that purpose and (3) do the individual's rights override the legitimate interest.
Responding to other rights in the GDPR	ICO consultation on guidance for subject access requests. ICO guidance for managing individual rights in a Big Data context.	No	Guidance on other rights in the GDPR can be informative but do not provide direct parallels with the RtbF. For example, subject access requests do not involve the same balancing test.

Drawing on the range of guidance above, it appears that:

1. A legitimate interest must be clearly articulated, real and present. Speculative or vague interests are not valid.
2. Legitimate interests are potentially broad. Examples include conventional marketing, prevention of misuse of services and research (including for marketing purposes). Although the grounds may be broad, the processing allowed by any interest is not and must be strictly necessary for that interest.[8]
3. If they appear equal, privacy rights generally trump legitimate interests. For legitimate interests to outweigh privacy rights, those privacy rights must clearly be more trivial. Evaluating this is the *balancing test.*
4. Factors to consider in the balancing test include:
   - Whether the legitimate interest is also a public interest
   - Quantity and level of invasiveness of data gathering
   - Potential for adverse results on the data subject (e.g., damaging reputation, negotiating power or autonomy, exclusion, discrimination or defamation) and emotional impacts (e.g., irritation, fear and distress)
   - Likelihood of risk materializing, and severity if it does
   - The result of the balancing test can, in some instances, be changed by implementing appropriate mitigating safeguards, including pseudonymization and other anonymization techniques.

What is Pseudonymization?

The GDPR defines pseudonymization as processing personal data such that the data can no longer be attributed to an individual without the use of additional information. Pseudonymization is often achieved by removing direct identifiers, such as a name or email address, and replacing them with a pseudonym. This process is also known as data masking or tokenization. For example, in a simple table of names and test scores replacing the names with randomly generated ID numbers, then storing the list of names and associated ID numbers in a separate table, would mean that the table containing ID numbers and test scores would be pseudonymous data.



[8] Note the Dutch data protection authority's decision of 3 March 2020. This goes against the established view that legitimate interests include commercial interests. It is subject to appeal at the time of writing.

How Should Organizations Manage RtbF Requests?

Managing RtbF requests can be challenging. Data about an individual may be distributed and simply deleting data can reduce the value of a dataset. For organizations using pseudonymous data, severing the link between the data and the individual may provide an attractive route to compliance.

The RtbF stems from an individual's right to privacy. Addressing the privacy risk can be more beneficial than simply deleting data. The privacy risk posed by processing can be mitigated in a number of ways, such as:

- Restricting access to the data
- Increasing data security through measures such as encryption at rest
- Protecting privacy through pseudonymization or anonymization.

In modern data ecosystems, identifying and deleting all the data relating to a specific individual may be difficult and have a high associated resource cost. This is particularly true of environments using Hadoop or the cloud, where data about an individual may be widely dispersed. As well as being technically challenging, deleting the data will reduce the value of the dataset, because it removes information that may be helpful for analysis. Therefore, organizations have an incentive to preserve that data.

We recommend that organizations implement privacy by design, including by processing pseudonymized data where possible. This can enable compliance with Articles 25 and 32 of the GDPR, which require that controllers take steps to integrate safeguards into their processing. Article 25 specifically mentions pseudonymization as an example. Pseudonymization and provides a baseline level of protection for all individuals whose data is processed and can also facilitate compliance with RtbF requests.

For example, pseudonymization requires that an individual cannot be identified without the use of additional data. This can be achieved by replacing direct identifiers (e.g. name, customer ID number, etc.) with pseudonyms. In some cases, the relationship between an individual and the pseudonym is stored separately in a 'dictionary'. Without access to the 'dictionary' it would be difficult to identify an individual based on the pseudonymous data.

In response to a RtbF request, the controller could delete the 'dictionary' entry relating to the individual who has made the request. That could have the effect of putting the data 'beyond use' as defined by the ICO and therefore complying with the RtbF request.[9]

How De-Identifying Data Can Strengthen Compliance with the GDPR

The Austrian Data Protection Authority's decision of 5/12/2018[10] involved a complaint brought by an individual against an organization which had taken steps to put the individual's data beyond use, including replacing some direct identifiers (e.g., name) with pseudonyms and deleting others (e.g., email address). It was no longer possible to search for the individual in the organization's systems. The individual argued that those steps were insufficient. The data protection authority disagreed. It found that deletion is not defined in the GDPR, that redaction is sufficient and that the organization had complied with the RtbF request by severing the link between the individual and the data.

[9] ICO, Deleting personal data. Note that severing the link between the individual and the data is only one element of putting the data beyond use.
[10] Austrian Data Protection Authority, decision DSB-D123.270 / 0009-DSB / 2018

Organizations Should Consider the Following Steps when Developing an Approach to the RtbF:

1. Carry out the balancing test. Before processing data, make sure your processing is legitimate. Pseudonymization may make processing, which would otherwise represent a risk to individual privacy, acceptable. This helps with the balancing test initially by reducing the risk posed to the individual and supports compliance with Articles 25 and 32 of the GDPR.
2. Evaluate the RtbF request. Bear in mind that the RtbF is not absolute and that the action needed depends on the legal basis for the processing. For example, controllers may have grounds to reject the request or the RtbF may not be applicable.
3. Instead of deleting the pseudonymized data, delete the dictionary entry. Deleting the individual's entry in the file storing the relationship between the pseudonyms and the individuals makes it unlikely that they will be identifiable in the future by the controller, potentially meeting the RtbF requirement.

It is important to note that whether or not this approach is appropriate will depend on factors such as the other variables in the data set, the strength of the legitimate interest and the potential privacy risk to the individual.

RtbF Action Plan

If you're planning for RtbF requests, we recommend considering the following:

1. Map your data processing to understand what data you have and what you are using it for. Delete, and do not collect, any data you do not need.
2. Can your business accomplish its objectives using anonymized or pseudonymized data? If you can, you should do so. This will both protect individual's privacy and give you more options for managing RtbF requests.
3. What are your grounds for processing? Carry out the balancing test for any legitimate interests or public interests, mapping your position for possible scenarios.
4. Consider a range of potential objections and RtbF requests and carry out the balancing test to see if you think you would need to comply, before or after any further mitigations.
5. Use this thought exercise to draft a framework for how you might respond to different groups of requests, and then seek legal advice to see if they agree with your framework. Google has a review board that looks at difficult cases. For most requests they are able to match the request to a known type and, therefore, a known response. This preparation makes it easier for them to manage the requests, and ensures all applicants are treated the same way.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136
US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal
www.privitar.com