WHITE PAPER

HOW TO QUALIFY DATA SUBJECTS FOR DATA DELETION?

Abstract

Data deletion is one of the common requirement which is part of privacy regulations. Both GDPR and CCPA, the two most recently introduced privacy laws provides data subjects with right to be forgotten. The legal definition of CCPA or GDPR defines data subjects as natural person who is resident of California or EU. The dilemma which arises for the organizations from the given legal construct is whether to process all data deletion requests or segregate and process resident specific requests. For instance, there is a huge multinational company having its operations in California, Australia, Europe, organization receives two data deletion request, one from Europe resident and other from Australian resident, the question now arises is that how to process these two requests? The white paper focuses on challenges related to data deletion, various approaches for processing data deletion requests and pros & cons associated with each approach. The white paper will elaborate on approach taking GDPR and CCPA as representative example but the approaches can be applied across other privacy regulations.

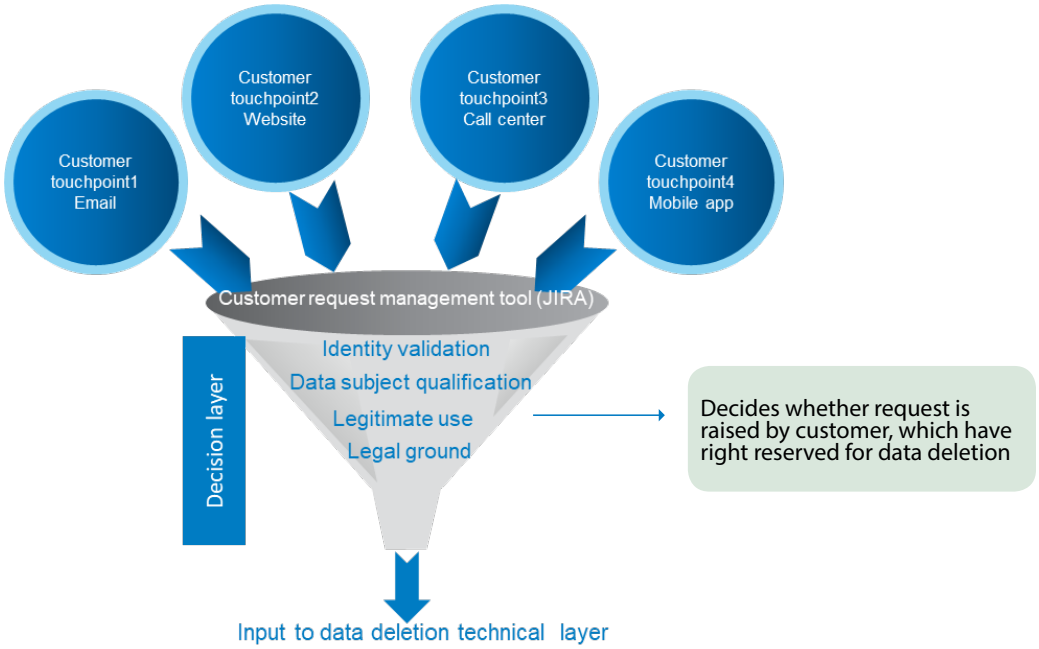
Infosys®
Navigate your next

Technical challenges and business implications

GDPR regulation applies to natural person who is resident of EU, similarly CCPA applies to natural person who is resident of California. These are legal definitions, but practical implementation of these has various technical challenges and business implications. Looking from the database point of view, it is very difficult to determine who is resident of EU/California and who is not. Building a rule engine which accurately and consistently identify the data subject's residence is a daunting task. Also any flaw in the rule engine can have legal implications, resulting in fines for noncompliance with privacy laws. On the other hand, looking from business point of view, if we delete all customer records business revenue's might take a hit.

Introduction to data deletion approach

Data deletion process diagram typically consists of customer touch points, customer request management tool which records all the deletion requests and manages the workflow; decision layer which finally decides which request needs to be sent for deletion and finally, technical layer for data deletion execution.



The subsequent section will focus on various approaches which organization can take for data subject qualification, each approach has pros and cons associated with them which is also elaborated in the subsequent section

Approaches for data subject qualification

Approach 1: Pre-tag customer data which belong California Residents

In the given approach, data subject qualification rule engine would create a separate tagging for California resident customers. Organization can achieve this objective by following below steps:

1. Map the customer journey
2. Identify what all attributes of a customer are being captured in the customer journey
3. Identify location and citizenship specific attributes and assess data quality of the attributes
4. Tag a customer using combination of attributes and test accuracy of tagging created from rule engine

The process becomes simpler for the organization which has invested in creating single customer view. Organizations which have attained that maturity, needs to focus on steps 3 and 4. Also, the key to the whole process is the quality of the data attributes which are being used to generate tag.

The below table provides industry wise view on what information is captured by specific industries, which can be used to tag customers.

Industry	Information captured	Customer Journey Stage	Accuracy
Banking	Residential proof Tax information	KYC (Customer acquisition) Tax payment records (Usage)	High
Insurance	Residential proof	KYC (Customer acquisition)	Medium
Telecom	Residential proof Geo Location tagging	CAF (Customer acquisition) CDR Data (Usage)	Medium
Retail	Delivery address Store purchase data External data	Order History(Purchase)	Low

The above approach will help organizations to retain high value customer profiles which do not fall under preview of privacy laws. Apart from retaining high value data, organizations taking the above approach can reap in the benefits of program in core business, as this can be a starting point for organizations to create a single customer view which can help them to get seamless customer experience across channels. The program would also test the quality of data on which current business decisions are taken and hence can improve overall information quality.

The downside of the approach is that, to miss on the legitimate customer request, if the tagging done to qualify request has some faults. Also the approach would need organizations to put in continuous efforts as this is not just one-time activity. Every time organization make new customer acquisition or imports new customer data from 3rd party, efforts will be needed to create tagging for new data sets. Also, the given approach will need significant implementation cost as this will impact existing data model.

Approach 2: Qualify the request at source

As an alternative to the approach 1, some of the organizations are considering to qualify data request right at the source of request. This can be done by taking an undertaking from customer that he is resident to geography where privacy law applies. This undertaking can be re-verified by IP address analysis. In case IP does not belong to geography, a further query can be raised to customer to provide additional document. The above approach is very simple and straight forward to implement. The downside of the approach is, deletion process will need more human intervention and hence would need higher human efforts in case of query.

Approach 3: Treat all request as same

The most conservative approach which organization can take is to treat all data deletion requests as same. In this particular approach if the request passes identity validation (i.e. requestor is the same person or have legal rights to ask for deletion for data subject mentioned in request), then organizations might not check the residency status. For example, a non-California resident requests for deletion, the organization opting for the approach will delete the data, though it is not required to do so under CCPA. The approach avoids implementation complexity and risk of missing out on legitimate request, but the drawback of this approach is organization will miss on opportunity to retain high value customer data.

Conclusion

The basic parameters which organization need to consider while finalizing the approach are:

- Territory of operations: If organization operates and own majority of customer data for geographies which are covered by privacy law than organization would have inclination towards approach 3
- Cost associated with failure vs value derived from data: Organizations should evaluate what penalty they might need to pay for missing on legitimate request vs value they derive from data. It has been observed that some organizations can lose 10-20% of their revenue due to data deletion and opt-out. This revenue loss is much higher when we put together cost of implementation and fines. Thus such organizations can evaluate solution 2 or solution 1 first. Decision between solution 1 and solution 2 will also depend on quality and type of data organization has.

There are various other parameters like time for implementation, data quality, expansion plans, complexity of data landscape which organization should also consider while evaluating each approach. Infosys has helped its client to identify best fit approach for them, using Infosys prioritization framework. The parameters which are considered in the framework includes data quality, risk associated with non-compliance, value derived from the customer personal data and complexity of implementation.

During certain engagements it has been observed that some of the organizations go for hybrid approach with objective to hedge the risk. Organizations at times intend to opt for approach 1 but initially start with approach 3, due to lack of implementation time. Infosys has helped the clients in such scenarios by creating roadmap and achieved desired level of maturity using phased approach.

About the Authors

Rohan Kanungo

Principal Consultant at Infosys

Rohan Kanungo is a Data Analytics & Data Privacy & Protection Consultant with 14+ years experience in IT Consultancy & Advisory services, BI Blue Printing & Org Design, BI Assessment, Strategic Transformation initiatives & Program Management. He has extensive experience in working with leading organizations in the areas of Information Management, Data Governance, Data Architecture, Data Strategy. What's been keeping him busy recently is enabling organizations in the area of data privacy and security by providing strategy & advisory services, crafting frameworks, solutions, service offerings, catalysts and accelerators. He can be reached at rohan.kanungo@Infosys.com

Anusha Tripathi

Principal Consultant at Infosys

Anusha Tripathi is a Data Analytics & Data Privacy & Protection Consultant with 16+ years experience in IT Consultancy & Advisory services, BI Assessment, Strategic Data Transformation initiatives for Data Insights. She has extensive experience in working with leading organizations in the areas of Information Management, Data Governance, Data Architecture, Data Strategy. What's been keeping her busy recently is enabling organizations in the area of data privacy and security by providing strategic guidance & advisory services. Enabling organizations by leveraging frameworks (CCPA & GDPR Enabled), implementing security solutions (RSA) and third party offerings and accelerators (One Trust). Reachable at Anusha_tripathi01@Infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next