International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Efficient Practices for Managing CCPA and GDPR Requests in Organizations

Rameshbabu Lakshmanasamy

Senior Data Engineer, Jewelers Mutual Group

Abstract: ***This article outlines good practices and implementation techniques of handling and honoring the CCPA (California Consumer Privacy act) or GDPR (General Data Protection Regulation) requests that nowadays have become a norm in many organizations. Only a handful of organizations are better prepared to handle this with seamless processes and collaboration of various teams with a product owner driving this effort clueless scrambling in dark. Listing out some good practices and how to manage such frequent requests with very minimal impacts on our day to day other ongoing priorities. A comprehensive fool proof process and understanding is needed as this comes with a hard deadline from legal standpoint. We can see these requests are incrementally growing month on month (if not weekly), and it is very important to have an automated or at least semi - automated procedures. This is important because the customer information are also buried in various touchpoints in the data pipeline right from the point - of - sale entry, operational systems to downstream reporting applications.***

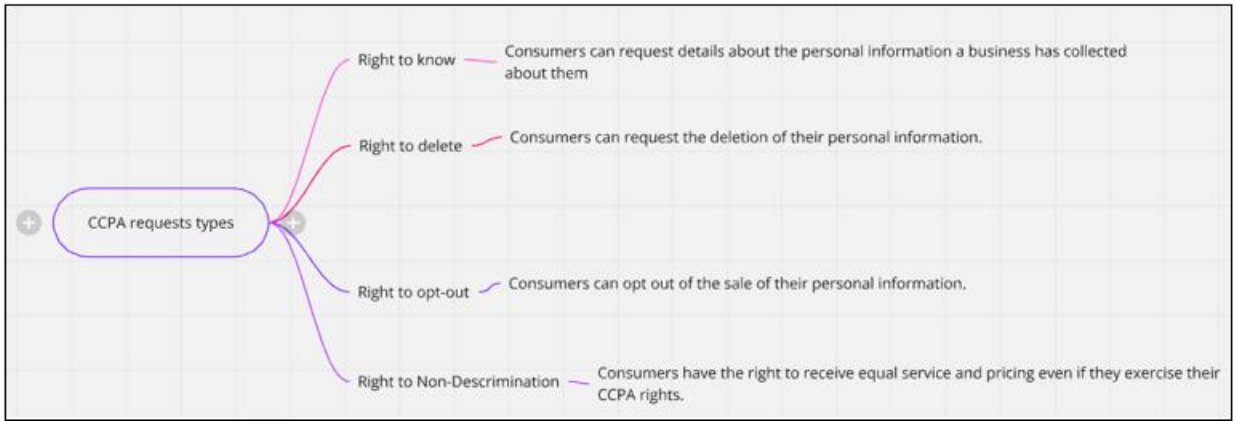
Keywords: CCPA, GDPR, Compliance, Govt regulation, Stakeholders collaboration, Automation, Best practices.

1. Introduction

In this digital era, it has become a norm to receive customer - requests to delete their information from IT systems of an organization. Meaning, any information stored in any storage or databases, irrespective of structured or unstructured, it should not be traceable back to the customer. This one line request have very high importance and weightage overriding any other high priority ongoing work, as these requests have legal compliance deadline, failing which it would cost the organization dearly. We will discuss here on identification of customer records, type of data strategy to adopt, collaborating between teams on finding the perfect sequence to accomplish this cleansing effort.

Customers are increasingly beware of their information available everywhere online, and worried about their privacy, and protection of their personal and sensitive data. They have started taking advantage of the government regulations such as CCPA or GDPR, to help limit their data expose. Once customer sends these type of requests, the IT Leadership are nervous and showing knee - jerk reaction due to nature of these requests that would endup in lawsuits, if not handled right. IT Leaders are getting matured slowly with experience on streamlining the processes and comprehensive best practices that will help them accomplish these requests precisely and on - time.

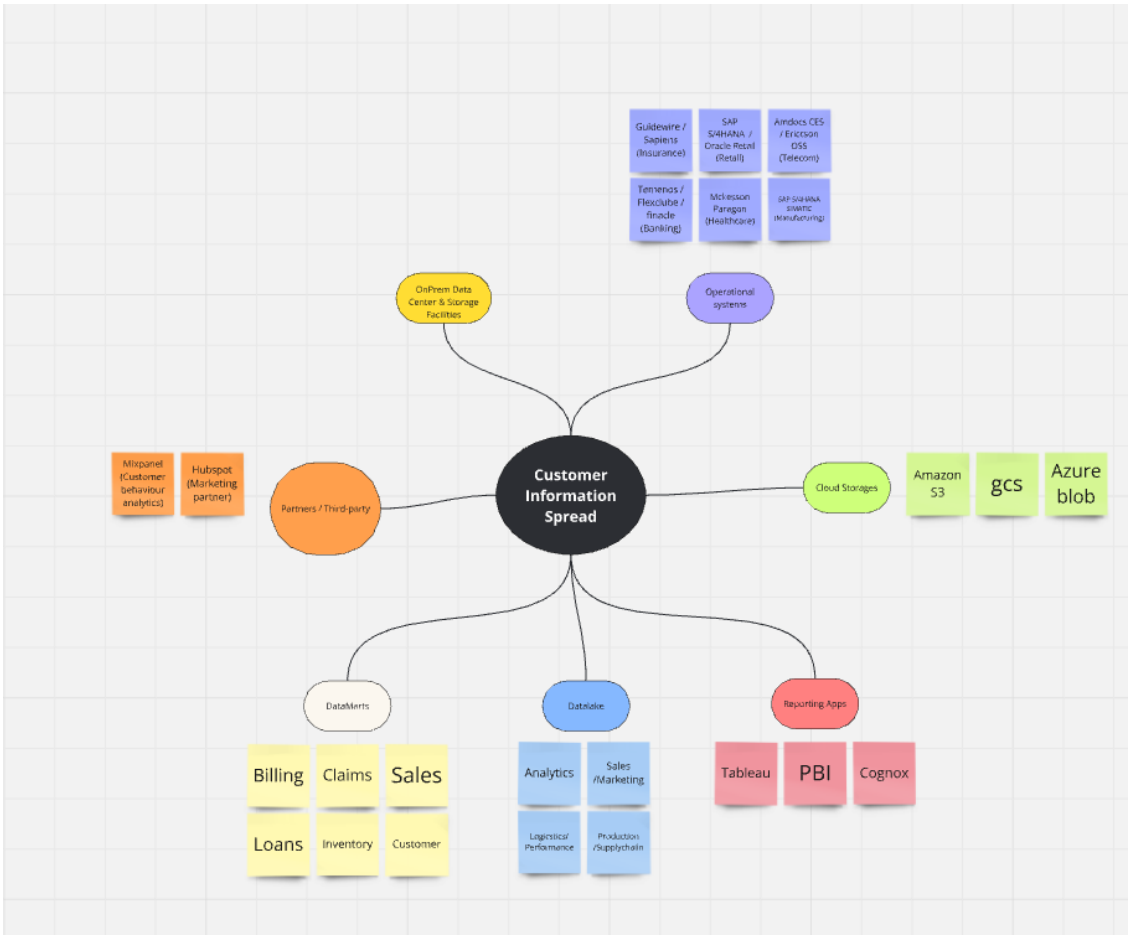
CCPA types:
Below chart outlines the possible types of requests that Corporations would get and description of each.



Process setup:
Team formation: It is important to designate a team that will comprise members from various applications to work in tandem, with ownership of cleansing in their own respective systems they are part of.
Acknowledgement: Send an acknowledgement to the requestor within 10 days of getting the request.
Game - plan: Have a clear game - plan/strategy to honor this request within 45 days. Narrow down the risk zones.

Identification:
On - Prem/In - house: The customer data can be existing in the point - of - sale operational systems, legacy applications, on premises storages.
Cloud: cloud storages like S3, GCS, Azure BLOB, Data Lake, datalakehouse, data warehouse, DataMart, reporting applications.
Third - Party/Partners: The data might be lying in third party partners/vendors like Mixpanel, Hubspot, Google analytics etc. It is very important to get the big picture of end to end

pipeline of data flow from entry to downstream system including the external partners. The third party partners can be at the point of entry sometimes, or at the extreme down end, and it is important to have that information to formulate a good strategy.



Data Strategy

Once we have identified the customer records in all the systems/locations, then we must know/decide on what type of data cleansing strategy to adopt. Is it one - size - fits - all type or unique to different applications/systems? What kind of data obfuscation to adopt – Data Masking, Tokenization, Data Encryption, Substitution, Data Redaction, Data Anonymization. This now comes to the discretion of the department leaders. Most teams would be okay with Data deletion, but marketing/sales teams would prefer to retain the records for historical statistics, and they would prefer Data Masking or Data Substitution strategies. It is very important to note that, whatever strategy adopted, the bottomline/goal is that the customer should not be traceable to from the data. With that goal in mind, management can adopt the strategy that aligns with their business goal.

Data Masking: In this model, all sensitive and personal information are replaced with fictional but realistic - looking data. E. g. SSN will be like *** - ** - 1234.

Data Substitution: Here, the original data is replaced with other values with similar format, but do not represent actual data. For e. g. we replace phone numbers with randomly generated numbers in same format.

Data Perturbation: This is altering the values slightly to prevent exact values from being identified at the same time the overall patterns to be analyzed.

Data Anonymization: This is where all identifying attributes are removed from datasets, retaining other attributes that doesn't trackback to the customer.

Data Deletion/Purging: In this mode, we will simply delete the customer records/row totally from the datasets. Not all teams would agree to this model.

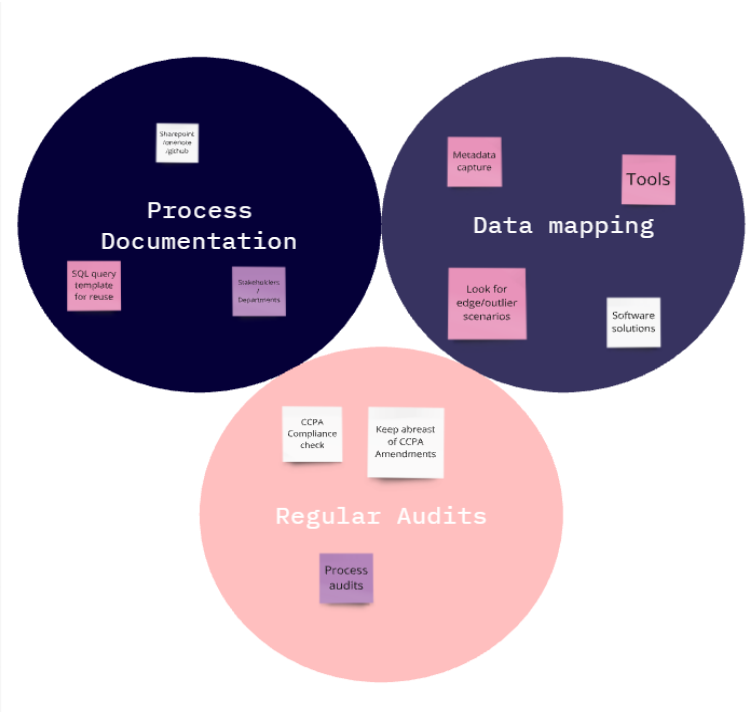
Among the above listed models of data cleansing, we may choose what best suits the team. Operational teams may be ready to part ways with the data, and would gladly go with data deletion. At the same time, the marketing/analytics team would want those records, and would simply prefer to adopt the anonymization or substitution that would help them retain those records for analytical activities without compromising the end goal of customer to be untraceable from the information available.

Documenting Learnings:

Records maintenance: All such requests maybe documented and kept for the period of 24 months including the responses. And regular audits to ensure CCPA compliance as well.

Process Documentation: Document/List all departments/ systems impacted and steps performed for the data cleansing. This may be GitHub - wiki, OneNote, SharePoint or whatever the standards being followed. Capture all the queries adopted for data masking or data anonymization for re - use for future requests.

Data Mapping: Identify and categorize all the sensitive information in your systems. This is a very important metadata for impact analysis and in the identification phase. This helps in automating such requests via software solutions/tools to streamline the handling of future requests.



References

[1] (2024) A General Information about the CCPA regulations. What are CCPA rights.
[2] https: //oag. ca. gov/privacy/ccpa#sectiona.
[3] Why your CCPA rights are important ? Who and What the CCPA covers https: //www.consumer - action. org/modules/articles/CCPA - Privacy - Rights
[4] Techniques to implement the data masking successfully: https: //satoricyber. com/data - masking/data - masking - 8 - techniques - and - how - to - implement - them - successfully/
[5] General Data Protection Regulation (GDPR) privisions, principles: https: //gdpr. eu/tag/gdpr/
[6] Data obfuscation techniques explained: https: //www.crowdstrike. com/cybersecurity - 101/data - obfuscation/