HANDLING REQUESTS FROM DATA SUBJECTS

Abstract

One of the biggest changes under different data privacy regulations is that data subjects will have extensive rights to their personal data. It is the controller's responsibility to facilitate the exercise of these rights which are listed below: Rights to Access, Rectify, be Forgotten, Restrict Processing, Portability, Object and Rights in relation to automated decision making and profiling. This POV provides a guideline on how to set a process for handling such requests.

Infosys®
Navigate your next

Table Of Contents

Formulating a strategy to address the influx of data subjects' requests

At a very high level, an organization can formulate the following plan to counter and address the data subjects' requests, which are expected to increase by a considerable amount after different data privacy regulations are gaining momentum across the world.

Identifying the touchpoints:

An organization needs to identify the various touchpoints for its data subjects to request for their data. Broadly, across organizations, there are 3 such touchpoints:

a) Profile or Account page (if available) which generally contains the following set of information:

  • PII present: Name, Email ID, Mobile number, Date of Birth, Address details, Order details (if any), Subscription history (if any).

  • Date of birth, Email ID, Mobile number, Address and Subscription can be edited.

  • The account can be deleted altogether

  • Profile page is available only for Registered users

  • For guest user, only Email ID and Mobile number are present. There is no profile page.

b) Consumer Care Service (email, chat, phone, etc.)

c) Consumer Privacy SPOC from the legal team of the organization (email)

Validate the data subject's identity:

Before proceeding with the request, the data subject's identity needs to be validated so that the data does not fall in the wrong hands, thus avoiding any data breach. This can be ensured by various methods which are described in the subsequent sections

Fulfilling the request:

Post validation, the organization must set up a set of well-defined process to honour the request from the data subject. This can be done in one of the three methods, which are described in more details in the subsequent sections of this POV:

a) Self fulfillment through Profile page

b) Customer Care/Central Operations team handling pre-defined requests independently without involvement of any legal SPOC

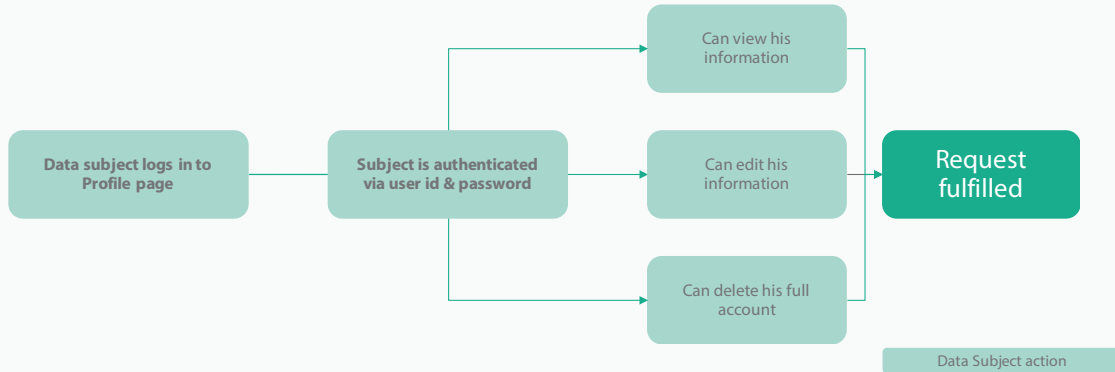c) Ad hoc requests necessitating involvement of the legal SPOC from the Consumer Privacy team

Detailed process flow

Touchpoint: Profile or Account page

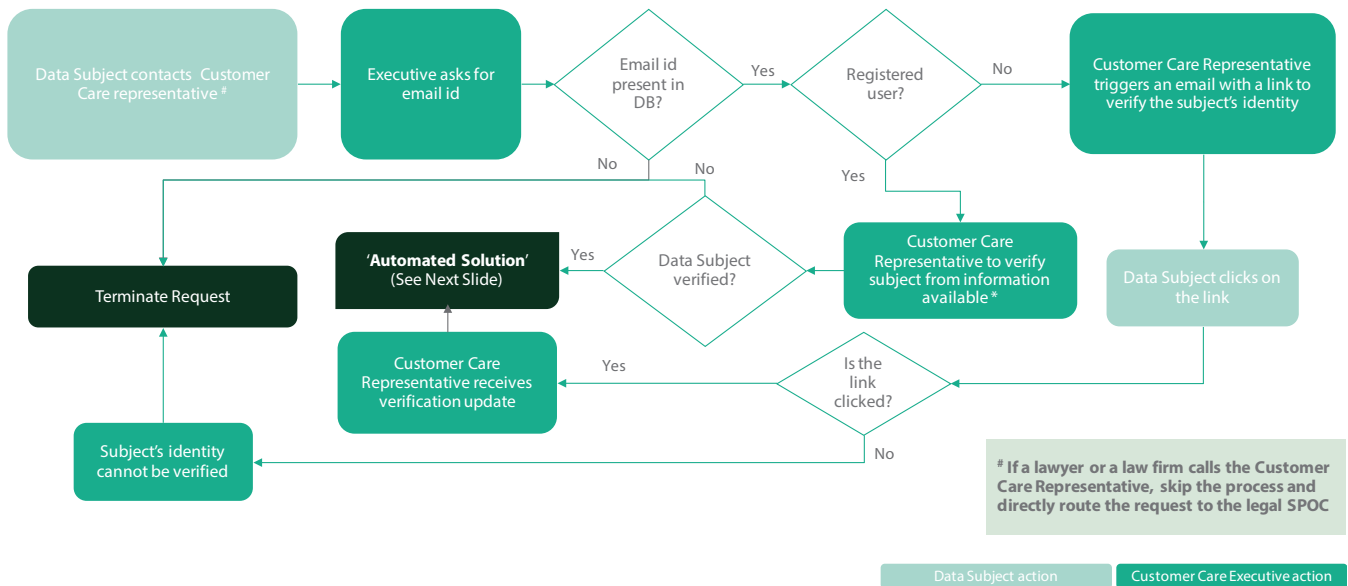This is the simplest method of fulfilling a request from data subject.

The identity is already validated through the username and password. Since the individual can edit the required fields, remove his account altogether

etc., these require almost zero participation from anyone in the organizations. Following is a schematic diagram of the process flow:

```
Data subject logs in to    →    Subject is authenticated    →    Can view his information
Profile page                    via user id & password      →    Can edit his information    →    Request fulfilled
                                                             →    Can delete his full account
```

Data Subject action

Touchpoint: Consumer Care Service

A data subject may get in touch with the consumer care service through email, phone, chat. In either case, the identity of the subject needs to be verified before routing the request to the appropriate teams in the organization. Following process flow illustrates a sample method of how to verify the identity:

```
Data Subject contacts Customer Care representative #  →  Executive asks for email id  →  Email id present in DB?  →Yes→  Registered user?  →No→  Customer Care Representative triggers an email with a link to verify the subject's identity

Email id present in DB? →No→ Terminate Request
Registered user? →Yes→ Customer Care Representative to verify subject from information available *

Data Subject verified? →Yes→ 'Automated Solution' (See Next Slide)
Data Subject verified? →No→ (Terminate Request)

Customer Care Representative receives verification update →Yes→ Is the link clicked?
Is the link clicked? →No→ Subject's identity cannot be verified → Terminate Request

Data Subject clicks on the link
```

If a lawyer or a law firm calls the Customer Care Representative, skip the process and directly route the request to the legal SPOC

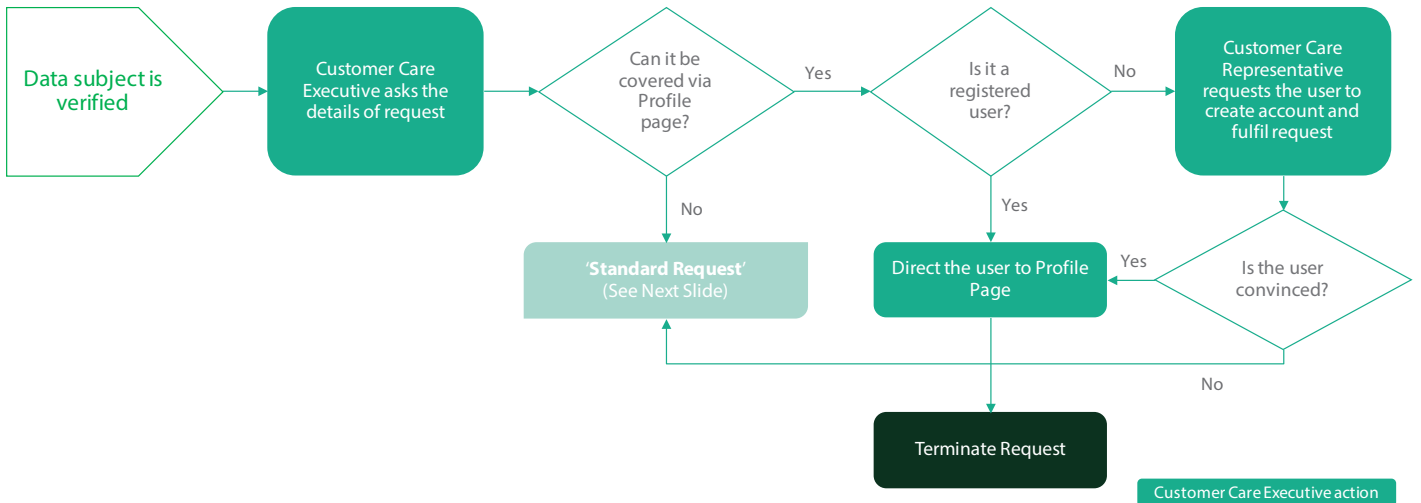Data Subject action   Customer Care Executive action

Name, Email ID, Mobile Number, Date of Birth, Last Order Date, Last Order ID, Last Address of Delivery, Last Subscription Details etc.

Post the verification, the request can be fulfilled in one of the 3 methods, as discussed in the previous section.
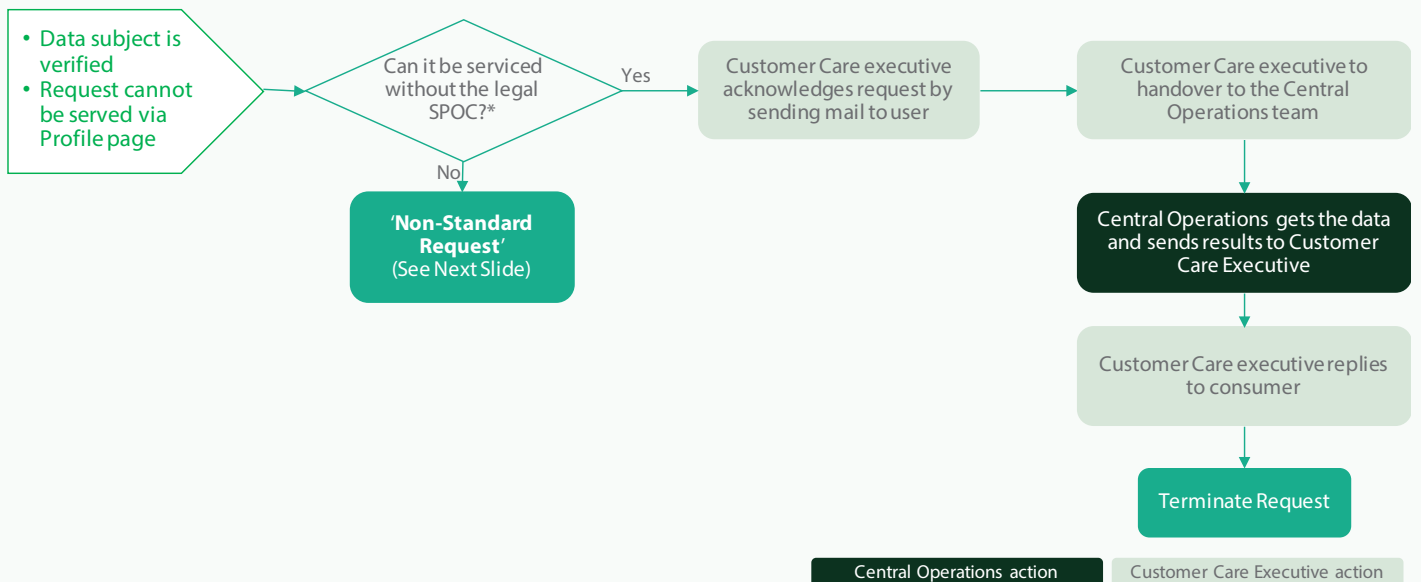
Fulfillment via profile page

These are the simplest requests which can be serviced by the Customer Care agents. The type of such requests are the ones which can be serviced from the profile/account page itself.

```
Data subject is        Customer Care          Can it be              Is it a           No    Customer Care
verified        →      Executive asks the  →  covered via   → Yes →  registered  →           Representative
                       details of request     Profile                user?                   requests the user to
                                              page?                                           create account and
                                                                                             fulfil request
                                                 ↓ No              ↓ Yes                           ↓
                                          'Standard Request'    Direct the user to Profile  ← Yes  Is the user
                                          (See Next Slide)      Page                               convinced?
                                                                      ↓                             ↓ No
                                                                Terminate Request
```

Customer Care Executive action

Fulfillment via Customer Care/Central Operations team for pre-defined requests
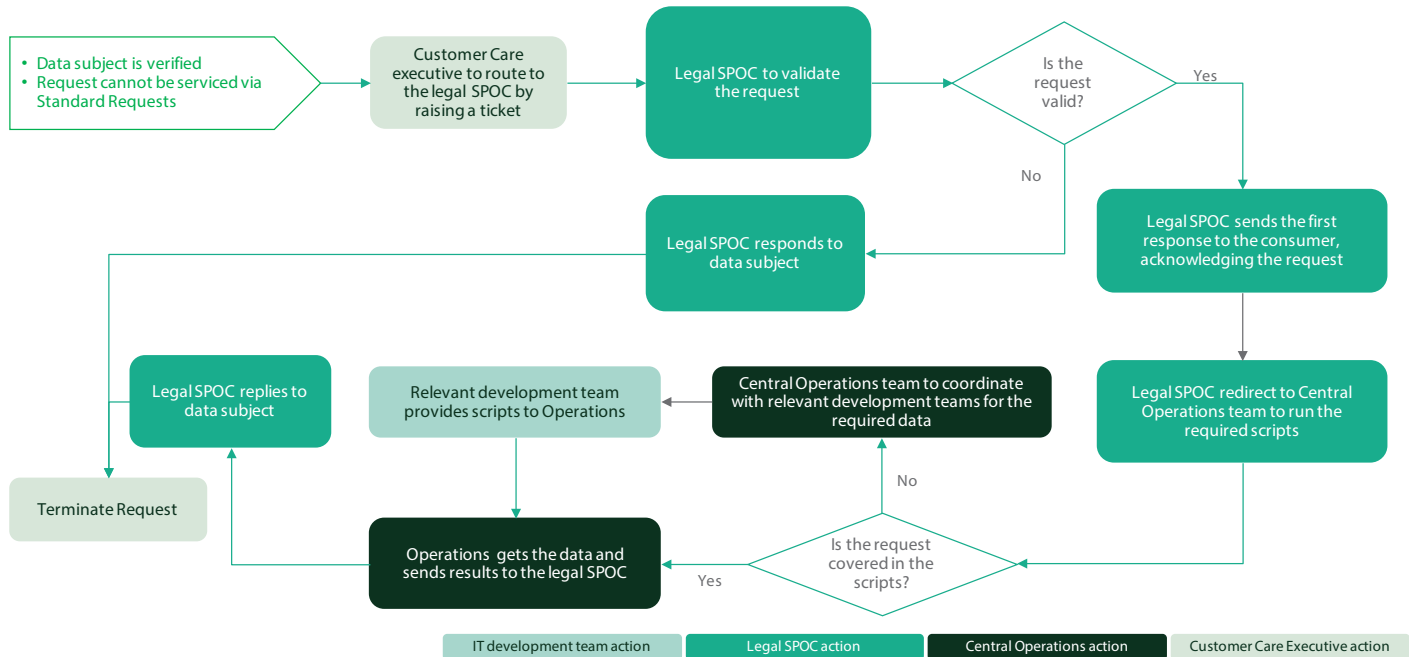
The organization needs to prepare a list of requests for which it can be beforehand. For such requests, the IT team can prepare scripts or queries well in advance and keep it ready to run and produce the results. The idea behind such request is to minimize the time of involvement from each team for every new request. This in turn leads to a better customer satisfaction as (s)he gets the data in a quick turnaround time.

```
• Data subject is       Can it be            Customer Care executive        Customer Care executive to
  verified              serviced      → Yes → acknowledges request by    →  handover to the Central
• Request cannot   →    without the legal    sending mail to user           Operations team
  be served via         SPOC?*                                                    ↓
  Profile page             ↓ No                                             Central Operations gets the data
                    'Non-Standard                                           and sends results to Customer
                    Request'                                                Care Executive
                    (See Next Slide)                                              ↓
                                                                           Customer Care executive replies
                                                                           to consumer
                                                                                 ↓
                                                                           Terminate Request
```

Central Operations action   Customer Care Executive action

Customer Care executive needs to develop a cookbook to handle the requests and in that document there should be a section to determine the types of requests that Customer Care representative can service without the involvement of the legal SPOC.

Fulfilment of ad hoc or unanticipated requests

There can be requests which are either unanticipated or are from an insisting client, who refuses to accept the response obtained in either of the above 2 steps. In such scenario, the request needs to be routed to the Consumer Privacy team of the legal unit, who takes the final decision in fulfilling it. Following flow chart describes this process.

- Data subject is verified
- Request cannot be serviced via Standard Requests

Customer Care executive to route to the legal SPOC by raising a ticket

Legal SPOC to validate the request

Is the request valid?

Yes

No

Legal SPOC responds to data subject

Legal SPOC sends the first response to the consumer, acknowledging the request

Legal SPOC replies to data subject

Relevant development team provides scripts to Operations

Central Operations team to coordinate with relevant development teams for the required data

Legal SPOC redirect to Central Operations team to run the required scripts

Terminate Request

Operations gets the data and sends results to the legal SPOC

Is the request covered in the scripts?

No

Yes

| IT development team action | Legal SPOC action | Central Operations action | Customer Care Executive action |

Touchpoint: Legal SPOC from the Consumer Privacy team

In some cases, the data subject may contact the Consumer Privacy team directly via email for exercising his/her rights. In such cases, the SPOC needs to fulfill the requests. While the SPOC is not on a live call with the data subject, the request can be forwarded to the Customer care agent and thus can be fulfilled in the methods described in the previous section. However, if he finds the request to be invalid, he can reject it outright and respond to the data subject accordingly.

Data Subject Rights and the Solution touchpoints

Among the rights that are made available to the data subject, some of them can easily be fulfilled by one or the other methods described in the previous sections. However, the organization may not be in a position to have pre-defined use cases for Rights to Restrict/Object Processing, Rights in relation to Automated Decision Making and Profiling. In such cases, the request must necessarily be routed through the legal SPOC. Following is a summary of how each right can be fulfilled by the solution touchpoints discussed above.

Consumer Rights	Through profile page	Through pre-defined steps	Through the legal SPOC
Right to Access	Yes	Yes	Yes
Right to Rectification	Yes	Yes	Yes
Right to Erasure	Yes	Yes	Yes
Right to Portability		Yes	Yes
Right to Restrict Processing			Yes
Right to Object Processing			Yes
Right in relation to Automated Decision Making and Profiling			Yes

Conclusion

Data privacy regulations places an utmost importance on the ownership of data. Data subjects are empowered with full rights to what to do with the data that a controller has about him/her. With this background, there is an expectation that the organizations will possibly experience an increase in the influx of requests from its customers. Hence, it is a good practice to set the procedures of how to respond to them. With the guidelines and procedures described in this POV, an organization can be at a vantage point where it will be one step ahead of its competitors in fulfilling its consumers' rights. This will help increase its image among its consumers and will foster its business in the process.

About the Authors

Parikshit Sharma
Principal Consultant at Infosys

Parikshit Sharma is a Data Governance & Data Privacy & Protection Consultant with 18+ 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 Enterprise Data Policy and Data Standards, Data Strategy & advisory services, Data Vendor Evaluations, Data solutions, service offerings, catalysts and accelerators.

He can be reached at Parikshit_sharma@Infosys.com

Anup Kumar Bose
Principal Consultant at Infosys, Member of International Association of Privacy Professionals (IAPP)

Anup is a Data Privacy, Governance and Management Consultant with more than one and half decade's experience in IT consultancy, advisory, marketing services, data org blue printing, BI assessment and development of product/service w.r.t. privacy issues. He has extensive experience in working with leading organizations in the areas of monitoring developments in regulatory and legislative change. In recent times Anup is enabling organizations to manage privacy issues working with privacy and data governance programs in the area of enterprise data policies, standards, lineage, strategy, advisory, vendor evaluations, solutions, service offerings, catalysts and accelerators.

He can be reached at anup_bose@Infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected   SlideShare